aws

Guia do usuário do ONTAP

FSx para ONTAP

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

FSx para ONTAP: Guia do usuário do ONTAP

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o Amazon FSx for NetApp ONTAP? ... 1
Características do FSx for ONTAP ... 2
Segurança e proteção de dados ... 3
Ferramentas de monitoramento ... 4
Preços FSx para ONTAP ... 4
FSx para ONTAP em AWS re:Post ... 4
Você é FSx usuário da Amazon pela primeira vez? ... 4
Como funciona ... 6
Sistemas de arquivos ... 6
Máquinas virtuais de armazenamento ... 6
Volumes ... 7
Níveis de armazenamento ... 7
Hierarquização de dados ... 8
Eficiência de armazenamento ... 8
Acessar seus dados ... 8
Gerenciamento de FSx recursos do ONTAP ... 9
Começar ... 10
Configuração ... 10
Inscreva-se para um Conta da AWS ... 10
Criar um usuário com acesso administrativo ... 11
Próxima etapa ... 12
Crie seu sistema FSx de arquivos para ONTAP ... 12
Como montar seu sistema de arquivos ... 16
Limpar os recursos ... 17
Regiões da AWS ... 19
Acessar seus dados ... 23
Clientes compatíveis ... 24
Usar protocolos de armazenamento em bloco ... 25
Acessando dados de dentro do Nuvem AWS ... 26
Acesso a dados da mesma VPC ... 26
Acesso a dados de uma VPC diferente ... 26
Acesso a dados de sistemas on-premises ... 30
Acessar endpoints NFS, SMB, da CLI e da API REST do ONTAP on-premises ... 31
Acesso a endpoints entre clusters de sistemas on-premises ... 32

Configurar o roteamento para acessar sistemas de arquivos Multi-AZ de fora de sua VPC 33
Configurar o roteamento para acessar sistemas de arquivos Multi-AZ on-premises 34
Montagem em clientes Linux 35
Como usar /etc/fstab para montar automaticamente na reinicialização da instância 36
Montagem em clientes Windows 38
Pré-requisitos 38
Montagem em clientes macOS 40
Provisionamento de iSCSI para Linux 43
Antes de começar 43
Instalar e configurar iSCSI no host Linux 45
Configurar iSCSI no sistema de arquivos FSx for ONTAP 46
Montar um LUN de iSCSI no cliente Linux 49
Provisionamento de iSCSI para Windows 55
Configurar o iSCSI no cliente Windows 56
Configurar iSCSI no sistema de arquivos FSx for ONTAP 57
Monte um LUN de iSCSI no cliente Windows 59
Validar sua configuração do iSCSI 63
Provisionamento NVMe /TCP para Linux 64
Antes de começar 65
Instale e configure NVMe no host Linux 66
Configurar NVMe no sistema de arquivos FSx for ONTAP 66
Monte um NVMe dispositivo em seu cliente Linux 69
Provisionamento para Windows NVMe/TCP 75
Acessar dados com outros serviços da AWS 75
Usando a Amazon WorkSpaces 75
Como usar o Amazon ECS 81
Usando o Amazon EVS 85
Usando a VMware nuvem 85
Opções de disponibilidade, durabilidade e implantação 86
Escolher um tipo de implantação do sistema de arquivos 86
Tipos de implantação Single-AZ 86
Tipos de implantação Multi-AZ 87
Escolher uma geração de sistema de arquivos 89
Processo de failover FSx para ONTAP 90
Como testar o failover em um sistema de arquivos 91
Recursos da rede 91

Sub-redes 91
Interfaces de rede elástica do sistema de arquivos 92
Performance 94
Avaliação da performance 94
Latência 94
Throughput e IOPS 94
Suporte para SMB Multichannel e NFS nconnect 95
Detalhes da performance 95
Impacto do tipo de implantação na performance 97
Impacto da capacidade de armazenamento na performance 100
Impacto da capacidade de throughput na performance 100
Exemplo: capacidade de armazenamento e capacidade de throughput 108
Administração de recursos 109
Como gerenciar a capacidade de armazenamento 109
Níveis de armazenamento 110
Escolha da capacidade de armazenamento do sistema de arquivos 111
Capacidade de armazenamento e IOPS do sistema de arquivos 116
Capacidade de armazenamento do volume 137
Gerenciar sistema de arquivos 163
Recursos do sistema de arquivos 164
Criar sistemas de arquivos 166
Atualizar sistemas de arquivos 181
Gerenciar pares de HA 184
Gerenciando o NVMe cache 194
Monitorar detalhes do sistema de arquivos 194
Excluir sistemas de arquivos 196
Gerenciando SVMs 196
Número máximo de SVMs por sistema de arquivos 197
Criando SVMs 198
Atualizando SVMs 204
Auditar acesso a arquivos 206
Configurar grupos de trabalho 218
Como monitorar detalhes da SVM 225
Excluindo SVMs 225
Como gerenciar volumes 227
Estilos de volume 228

Tipos de volume 230
Estilo de segurança do volume 231
Como criar volumes 232
Atualizar volumes 237
Mover volumes 241
Monitoramento de volumes 245
Excluir volumes do 247
Como criar um LUN de iSCSI 250
Próximas etapas 252
Atualizar janelas de manutenção 252
Como gerenciar a capacidade de throughput 253
Quando modificar a capacidade de throughput 255
Como as solicitações simultâneas são processadas 255
Atualizar a capacidade de throughput 256
Como monitorar as alterações na capacidade de throughput 257
Como gerenciar compartilhamentos de SMB 259
Gerenciando com NetApp aplicações 262
Inscrevendo-se para um NetApp conta 262
O uso do NetApp BlueXP 263
Usar o NetApp ONTAP CLI 264
Usar o ONTAP API REST 268
Marcar recursos 268
Conceitos Básicos de Tags 269
Marcando seus Recursos 270
Copiar tags para backups 271
Restrições de tags 272
Permissões e marcação de tags 272
Como proteger seus dados 273
Fazer o backup de volumes do 273
Como funcionam os backups 275
Requisitos de armazenamento 275
Backups automáticos diários 276
Backups iniciados pelo usuário 277
Copiar tags para backups 277
Usando AWS Backup 277
Como restaurar backups 278

Desempenho de backup 280
Fazer o backup de volumes do SnapLock 281
Como criar backups iniciados pelo usuário 282
Como restaurar backups 282
Restaurar um subconjunto de dados 286
Monitorando o andamento da restauração do volume 287
Excluir backups 289
Como usar snapshots de volume 291
Políticas de snapshots 291
Restauração de arquivos com base em snapshots 292
Visualizar o snapshot comum 293
Atualizar o espaço de reserva de snapshot 294
Desabilitar snapshots automáticos 295
Exclusão de snapshots 297
Exclusão de snapshots 298
Reserva de snapshot 299
Protegendo dados com a Proteção Autônoma contra Ransomware 300
Como funciona o ARP 300
O que o ARP procura 301
Como responder a um ataque suspeito com o ARP 302
Habilitando o ARP 303
Respondendo aos alertas do ARP 305
Entendendo os alertas do EMS para ARP 307
Protegendo dados com SnapLock 309
Como SnapLock funciona 309
Noções básicas SnapLock Compliance 314
Noções básicas SnapLock Enterprise 315
Entendendo o SnapLock período de retenção 316
Confirmar arquivos para o WORM 319
Replicando seus dados com FlexCache 324
Como a FlexCache funciona 324
FlexCachemodos de gravação 324
FlexCachevisão geral da criação de volume 325
Criação de um FlexCache 325
O uso do SnapMirror para replicação programada 331
O uso do NetApp BlueXP para programar a replicação 332

Usar o ONTAP CLI para programar a replicação ... 332
Relatórios de uso e faturamento ... 333
FSx para o relatório de cobrança do ONTAP ... 333
FSx para relatório de uso do ONTAP ... 337
Como monitorar sistemas de arquivos ... 342
Monitoramento com CloudWatch ... 343
Acessando CloudWatch métricas ... 344
Monitoramento no FSx console da Amazon ... 346
Métricas do sistema de arquivos ... 358
Métricas para sistemas de arquivos de segunda geração ... 382
Métricas de volume ... 400
Monitoramento de eventos EMS ... 409
Visão geral dos eventos EMS ... 410
Visualização de eventos EMS ... 411
Encaminhamento de eventos do EMS para um servidor Syslog ... 418
Monitoramento com insights de infraestrutura de dados ... 420
Monitorar com Harvest e Grafana ... 421
Conceitos básicos do Harvest e Grafana ... 421
Painéis compatíveis do Harvest ... 422
Sem compatibilidade Harvest painéis ... 423
AWS CloudFormation modelo ... 423
Tipos de EC2 instância da Amazon ... 424
Procedimento de implantação ... 424
Fazer login no Grafana ... 428
Solução de problemas do Harvest e Grafana ... 428
Monitoramento com AWS CloudTrail ... 432
FSx Informações da Amazon em CloudTrail ... 432
Entendendo as entradas do arquivo de FSx log da Amazon ... 433
Trabalhar com o Active Directory ... 436
Pré-requisitos do Active Directory autogerenciado ... 437
Requisitos para Active Directory autogerenciado ... 437
Requisitos de configuração de rede ... 438
Requisitos de conta de serviço do Active Directory ... 439
Práticas recomendadas de Active Directory autogerenciado ... 441
Delegando permissões à sua conta de FSx serviço da Amazon ... 441
Mantenha uma configuração do AD atualizada ... 442

Limite o tráfego em uma VPC com grupos de segurança ... 443
Como criar regras de saída de grupo de segurança ... 443
Como funciona SVMs a adesão ao Active Directory ... 443
Informações necessárias do Active Directory ... 445
Como gerenciar configurações do Active Directory para SVM ... 446
Ingressando SVMs no Active Directory ... 446
Atualizar configurações de Active Directory ... 450
Atualizando as configurações do Active Directory com a CLI NetApp ... 451
Migração para a Amazon FSx ... 457
Migrando usando SnapMirror ... 457
Antes de começar ... 459
Criar o volume de destino ... 461
Registre a origem e o destino entre clusters LIFs ... 462
Estabelecer o emparelhamento de clusters entre a origem e o destino ... 463
Criar um relacionamento de emparelhamento entre SVMs ... 464
Crie o SnapMirror relacionamento ... 465
Transfira dados para o seu sistema FSx de arquivos para ONTAP ... 465
Passando para a Amazon FSx ... 466
Migrando arquivos com AWS DataSync ... 468
Pré-requisitos ... 469
DataSync etapas básicas de migração ... 469
Segurança ... 470
Proteção de dados ... 471
Criptografia de dados FSx para ONTAP ... 472
Criptografia em repouso ... 472
Criptografia de dados em trânsito ... 474
Gerenciamento de identidade e acesso ... 496
Público ... 497
Autenticação com identidades ... 498
Gerenciar o acesso usando políticas ... 501
FSx para ONTAP e IAM ... 504
Exemplos de políticas baseadas em identidade ... 510
Solução de problemas do IAM ... 513
Uso de perfis vinculados ao serviço ... 515
Usando tags com a Amazon FSx ... 521
AWS políticas gerenciadas ... 527

Amazon FSx ServiceRolePolicy 528
Amazon FSx DeleteServiceLinkedRoleAccess 528
Amazon FSx FullAccess 528
Amazon FSx ConsoleFullAccess 529
Amazon FSx ConsoleReadOnlyAccess 530
Amazon FSx ReadOnlyAccess 531
Atualizações da política 531
Controle de acesso ao sistema de arquivos com a Amazon VPC 544
Grupos de segurança da Amazon VPC 544
Validação de conformidade 547
Endpoints da VPC de interface 549
Considerações sobre os endpoints VPC da FSx interface Amazon 549
Criação de uma interface VPC endpoint para a API da Amazon FSx 550
Criação de uma política de VPC endpoint para a Amazon FSx 550
Resiliência 551
Backup e restauração 551
Snapshots 551
Zonas de disponibilidade 551
Segurança da infraestrutura 552
Como usar software antivírus 553
Usuários e perfis do ONTAP 553
Perfis e usuários de administrador do sistema de arquivos 554
Perfis e usuários de administrador do SVM 555
Autenticação de usuários do ONTAP com o Active Directory 558
Criação de novos usuários do ONTAP para administração do sistema de arquivos e do SVM 558
Criação de usuários do ONTAP 559
Criação de perfis de SVM 562
Configuração da autenticação do Active Directory para usuários do ONTAP 564
Como configurar a autenticação de chave pública 566
Atualização dos requisitos de senha 567
Falha na atualização da senha da conta `fsxadmin` 568
Cotas 570
Cotas que podem ser aumentadas 570
Cotas de recursos para cada sistema de arquivos 572
Solução de problemas 578

Sistemas de arquivos configurados incorretamente 578
Compartilhamento de VPC desativado 578
Não é possível criar um sistema de arquivos Multi-AZ 579
Nível SSD com mais de 90% de capacidade total 579
Não é possível acessar o sistema de arquivos 580
Etiquetas de tabela de rotas ausentes 580
Muitas rotas 581
Rotas perdidas para os servidores 581
ENI modificado ou excluído 582
ENI excluído 582
Regras de entrada ausentes 582
Regras de saída ausentes 582
A sub-rede da instância de computação não usa nenhuma das tabelas de rotas associadas ao seu sistema de arquivos 582
Não é possível atualizar a tabela de rotas Multi-AZ 583
Não consigo acessar iSCSI 583
Sub-rede VPC não compartilhada 584
NFS, SMB, ONTAP CLI e API inacessíveis de diferentes VPCs e locais 584
SVM configurado incorretamente 584
Seu SVM tem um volume off-line 584
Seu SVM tem um volume off-line com um iSCSI LUN ou um namespace /TCP NVMe 585
Não consigo juntar SVM ao AD 585
Nome SVM NetBIOS igual ao domínio inicial 586
O SVM é unido a outro AD 587
Nome do SVM NetBIOS já usado 587
FSx não consegue acessar os controladores de domínio do AD 587
Configuração de porta ou permissões de conta de serviço insuficientes 588
Credenciais inválidos da conta de serviço 589
A Amazon não FSx consegue se conectar aos seus controladores de domínio do Active Directory devido à insuficiência de credenciais da conta de serviço 589
Não consigo acessar servidores AD DNS ou controladores de domínio 590
Nome de domínio AD inválido 592
A conta de serviço não pode acessar o grupo de administradores do AD 593
A OU especificada é inválida 593
Não é possível excluir o SVM ou o volume 594
Identificar falhas em exclusões 595

Exclusão de SVM: tabelas de rotas inacessíveis 595
Exclusão da SVM: relacionamento entre pares 597
SVM ou exclusão de volume: SnapMirror 598
Exclusão de SVM: LIF habilitada pelo Kerberos 599
Exclusão de SVM: outro motivo 601
Exclusão de volume: relacionamento FlexCache 603
Volume configurado incorretamente 604
Volume acima de 98% cheio 604
O volume de armazenamento em bloco está off-line 604
Off-line FlexCache volume de origem 605
Volume off-line com SnapMirror relação 605
O volume de armazenamento em bloco é restrito 606
Volume de FlexCache origem restrito 606
Volume restrito com SnapMirror relação 606
O volume tem armazenamento insuficiente 607
Determine como a capacidade de armazenamento do volume está sendo usada 607
Como aumentar a capacidade de armazenamento de um volume 608
Como usar o dimensionamento automático de volume 608
O armazenamento principal do sistema de arquivos está cheio 608
Exclusão de snapshots 608
Como aumentar a capacidade máxima de arquivos de um volume 609
Backups de volume com falha 610
Corrigir problemas de rede 610
Você deseja capturar um rastreamento de pacote 610
Histórico do documento 614
..... dcxxxvii

O que é o Amazon FSx for NetApp ONTAP?

O Amazon FSx for NetApp ONTAP é um serviço totalmente gerenciado que fornece armazenamento de arquivos altamente confiável, escalável, de alto desempenho e rico em recursos, baseado no NetApp popular sistema de arquivos ONTAP. FSx for ONTAP combina os recursos, o desempenho, os recursos e as operações de API familiares dos sistemas de NetApp arquivos com a agilidade, escalabilidade e simplicidade de um sistema totalmente gerenciado. AWS service (Serviço da AWS)

FSx for ONTAP fornece armazenamento de arquivos compartilhado rico em recursos, rápido e flexível que é amplamente acessível a partir de instâncias de computação Linux, Windows e macOS executadas no local ou no local. AWS FSx for ONTAP oferece armazenamento em unidade de estado sólido (SSD) de alto desempenho com latências de submilissegundos. Com FSx o ONTAP, você pode atingir níveis de desempenho de SSD para sua carga de trabalho enquanto paga pelo armazenamento SSD para apenas uma pequena fração de seus dados.

Gerenciar seus dados com o FSx for ONTAP é mais fácil porque você pode capturar, clonar e replicar seus arquivos com o clique de um botão. Além disso, o FSx for ONTAP classifica automaticamente seus dados em camadas em um armazenamento elástico de baixo custo, diminuindo a necessidade de provisionar ou gerenciar a capacidade.

FSx for ONTAP também fornece armazenamento altamente disponível e durável com backups totalmente gerenciados e suporte para recuperação de desastres entre regiões. Para facilitar a proteção e a proteção de seus dados, o FSx for ONTAP oferece suporte a aplicativos populares de segurança de dados e antivírus.

Para clientes que usam o NetApp ONTAP no local, o FSx for ONTAP é a solução ideal para migrar, fazer backup ou expandir seus aplicativos baseados em arquivos do local para AWS sem a necessidade de alterar o código do aplicativo ou a forma como você gerencia seus dados.

Como um serviço totalmente gerenciado, o FSx for ONTAP facilita o lançamento e a escalabilidade de um armazenamento de arquivos compartilhado confiável, de alto desempenho e seguro na nuvem. Com FSx o ONTAP, você não precisa mais se preocupar com:

- Configurar e provisionar servidores de arquivos e volumes de armazenamento
- Replicar dados
- Instalar e aplicar patches no software do servidor de arquivos
- Detectar e resolver falhas de hardware

- Como gerenciar o failover e o failback
- Executar backups manualmente

FSx for ONTAP também fornece uma integração avançada com outros AWS serviços, como AWS Identity and Access Management (IAM) WorkSpaces, Amazon, AWS Key Management Service (AWS KMS) e. AWS CloudTrail

Tópicos

- Características do FSx for ONTAP
- Segurança e proteção de dados
- Ferramentas de monitoramento
- Preços FSx para ONTAP
- FSx para ONTAP em AWS re:Post
- Você é FSx usuário da Amazon pela primeira vez?

Características do FSx for ONTAP

Com FSx o ONTAP, você obtém uma solução de armazenamento de arquivos totalmente gerenciada com:

- Suporte para conjuntos de dados em escala de petabytes em um único namespace
- Até dezenas de gigabytes por segundo (GBps) de taxa de transferência por sistema de arquivos
- Acesso multiprotocolo aos dados usando os protocolos Network File System (NFS), Server Message Block (SMB), Internet Small Computer Systems Interface (iSCSI) e Non-Volatile Memory Express () NVMe
- Opções de implantação Multi-AZ e Single-AZ altamente disponíveis e duráveis
- Classificação automática de dados em camadas que reduz os custos de armazenamento ao fazer a transição automática de dados acessados com pouca frequência para um nível de armazenamento de menor custo com base em seus padrões de acesso
- Compressão, eliminação de duplicação e compactação de dados para reduzir o consumo de armazenamento
- Suporte para NetAppde SnapMirror recurso de replicação
- Suporte para NetAppsoluções de armazenamento em cache local da: NetApp Global File Cache e FlexCache

- Support para acesso e gerenciamento usando o nativo AWS ou NetApp ferramentas e operações de API
  - AWS Management Console, AWS Command Line Interface (AWS CLI) e SDKs
  - NetApp CLI do ONTAP, API REST e BlueXP

Segurança e proteção de dados

O modelo de responsabilidade compartilhada é empregado no que se refere a. Segurança na Amazon FSx para NetApp ONTAP FSx A Amazon oferece vários níveis de segurança e conformidade para facilitar a proteção de seus dados.

FSx for ONTAP suporta os seguintes recursos de proteção de dados, segurança e controle de acesso:

- Criptografando dados em repouso para dados e backups do sistema de arquivos usando AWS KMS keys
- Criptografando dados em trânsito usando:
  - Kerberos para pequenas e médias empresas
  - IPSEC
  - Criptografia baseada em NITRO
- Escaneamento antivírus sob demanda
- Autenticação e autorização usando o Microsoft Active Directory
- Auditoria de acesso a arquivos
- NetAppSnapLockWORM com modos de conformidade e retenção empresarial

Para obter mais informações, consulte Proteção de dados na Amazon FSx para NetApp ONTAP e Como proteger seus dados.

Além disso, a Amazon FSx protege seus dados com backups altamente duráveis do sistema de arquivos. A Amazon FSx realiza backups diários automáticos, e você pode fazer backups adicionais a qualquer momento. Para obter mais informações, consulte Como proteger seus dados.

Ferramentas de monitoramento

As ferramentas de monitoramento incluem CloudWatchCloudTrail, ONTAP eventos do EMS, NetApp Insights sobre a infraestrutura de dados e NetApp Colheita.

Preços FSx para ONTAP

Você é cobrado pelos sistemas de arquivos com base nas seguintes categorias:

- Capacidade de armazenamento SSD (por gigabyte/mês ou GB/mês)
- IOPS de SSD que você provisiona acima de três IOPS/GB (por IOPS/mês)
- Capacidade de taxa de transferência (por megabytes por segundo [] MBps -mês)
- Consumo de armazenamento do pool de capacidade (por GB/mês)
- Solicitações de pool de capacidade (por leitura e gravação)
- Consumo de armazenamento de backup (por GB/mês)

Para obter mais informações sobre preços e taxas associadas ao serviço, consulte os preços da Amazon FSx for NetApp ONTAP.

FSx para ONTAP em AWS re:Post

Se você encontrar problemas ao usar a Amazon FSx, use AWS re:Postpara obter respostas às suas FSx perguntas do ONTAP.

Você é FSx usuário da Amazon pela primeira vez?

Se você é um usuário iniciante da Amazon FSx, recomendamos que você leia as seções a seguir na ordem:

1. Se você é novo em AWS, veja como Configurando o FSx ONTAP configurar um Conta da AWS.
2. Se você estiver pronto para criar seu primeiro sistema de FSx arquivos da Amazon, siga as instruções emComeçando a usar a Amazon FSx para NetApp ONTAP.
3. Para obter mais informações sobre performance, consulte Amazon FSx para desempenho do NetApp ONTAP.

4. Para obter detalhes FSx de segurança da Amazon, consulteSegurança na Amazon FSx para NetApp ONTAP.
5. Para obter informações sobre a FSx API da Amazon, consulte a Referência da FSx API da Amazon.

Como funciona o Amazon FSx for NetApp ONTAP

Este tópico apresenta os principais recursos dos sistemas de arquivos Amazon FSx for NetApp ONTAP e como eles funcionam, com links para seções com descrições detalhadas, detalhes importantes de implementação e step-by-step procedimentos de configuração.

Tópicos

- FSx para sistemas de arquivos ONTAP
- Máquinas virtuais de armazenamento
- Volumes
- Níveis de armazenamento
- Eficiência de armazenamento
- Acessando dados armazenados nos sistemas FSx de arquivos ONTAP
- Gerenciamento de FSx recursos do ONTAP

FSx para sistemas de arquivos ONTAP

Um sistema de arquivos é o principal FSx recurso ONTAP, análogo a um cluster ONTAP local NetApp . Você especifica a capacidade de armazenamento da unidade de estado sólido (SSD) e a capacidade de throughput do sistema de arquivos, além de escolher uma Amazon Virtual Private Cloud (VPC) na qual seu sistema de arquivos será criado. Para obter mais informações, consulte Gerenciamento FSx para sistemas de arquivos ONTAP.

Seu sistema de arquivos pode ter de 1 a 12 pares de alta disponibilidade (HA), dependendo da configuração. Um par de HA é composto por 2 servidores de arquivos em uma configuração de espera ativa. A primeira geração FSx para sistemas de arquivos ONTAP e os sistemas de arquivos Multi-AZ de segunda geração oferecem suporte a um par HA. Os sistemas de arquivos Single-AZ de segunda geração são compatíveis com até 12 pares de HA. Para obter mais informações, consulte Gerenciar pares de alta disponibilidade (HA).

Máquinas virtuais de armazenamento

Uma máquina virtual de armazenamento (SVM) é um servidor de arquivos isolado com seus próprios endpoints administrativos e de acesso a dados, para fins de administrar e acessar dados. Quando

você acessa dados em seu sistema de arquivos FSx for ONTAP, seus clientes e estações de trabalho interagem com uma SVM usando o endereço IP do endpoint da SVM. Para obter mais informações, consulte Gerenciando SVMs.

Você pode SVMs ingressar em um Microsoft Active Directory para autenticação e autorização de acesso a arquivos. Para obter mais informações, consulte Trabalhando com o Microsoft Active Directory no FSx ONTAP.

Volumes

FSx para ONTAP, os volumes são recursos virtuais que você usa para organizar e agrupar seus dados. Os volumes são contêineres lógicos hospedados em SVMs, e os dados armazenados neles consomem a capacidade de armazenamento físico em seu sistema de arquivos.

Ao criar um volume, você define o tamanho, o que determina a quantidade de dados físicos que podem ser armazenados nele, independentemente do nível de armazenamento de dados em que ele esteja armazenado. Você também define o tipo de volume, RW (leitura/gravável) ou DP (proteção de dados). Um volume DP é somente para leitura e pode ser usado como destino em um NetApp SnapMirror relacionamento. SnapVault

FSx para ONTAP, os volumes são provisionados de forma reduzida, o que significa que eles só consomem capacidade de armazenamento para os dados armazenados neles. Com volumes de provisionamento thin, a capacidade de armazenamento não é reservada com antecedência. Em vez disso, o armazenamento é alocado dinamicamente, conforme necessário. O espaço livre é liberado de volta para o sistema de arquivos quando os dados no volume ou no LUN são excluídos. Por exemplo, você pode criar 3 volumes de 10 TiB em um sistema de arquivos configurado com 10 TiB de capacidade de armazenamento livre, desde que a quantidade total de dados armazenados nos 3 volumes nunca exceda 10 TiB. A quantidade de dados armazenados fisicamente em um volume é contabilizada para o consumo geral da capacidade de armazenamento. Para obter mais informações, consulte Gerenciamento FSx de volumes ONTAP.

Níveis de armazenamento

Um sistema de arquivos FSx for ONTAP tem dois níveis de armazenamento: armazenamento primário e armazenamento em pool de capacidade. O armazenamento principal é um armazenamento SSD provisionado, escalável e de alta performance, criado especificamente para a parte ativa do seu conjunto de dados. O armazenamento do grupo de capacidade é um nível

de armazenamento totalmente elástico cujo tamanho pode ser escalado para petabytes, sendo otimizado em termos de custo para dados acessados com pouca frequência. Os dados gravados nos volumes consomem capacidade nos níveis de armazenamento. Para obter mais informações, consulte FSx para níveis de armazenamento ONTAP.

Hierarquização de dados

A classificação por níveis de dados é o processo pelo qual o Amazon FSx for NetApp ONTAP move automaticamente os dados entre o SSD e os níveis de armazenamento do pool de capacidade. Cada volume tem uma política de camadas que controla se os dados são movidos para o nível de capacidade quando ficam inativos (frios). O período de resfriamento da política de camadas de um volume determina quando os dados se tornam inativos (frios). Para obter mais informações, consulte Divisão de dados em níveis no volume.

Eficiência de armazenamento

O Amazon FSx for NetApp ONTAP oferece suporte aos recursos de eficiência de armazenamento em nível de bloco do ONTAP — compactação, compactação e desduplicação — para reduzir a capacidade de armazenamento que seus dados consomem. Os recursos de eficiência de armazenamento podem reduzir o espaço ocupado pelos dados no armazenamento SSD, no armazenamento do grupo de capacidade e nos backups. A economia típica da capacidade de armazenamento das workloads de compartilhamento de arquivos de uso geral, sem sacrificar a performance, é de 65% com compressão, eliminação de duplicação e compactação, tanto nos níveis de armazenamento SSD quanto no grupo de capacidade. Para obter mais informações, consulte Eficiência de armazenamento.

Acessando dados armazenados nos sistemas FSx de arquivos ONTAP

Você pode acessar seus dados FSx para volumes ONTAP de vários clientes Linux, Windows ou macOS simultaneamente por meio dos protocolos NFS (v3, v4, v4.1, v4.2) e SMB. Você também pode acessar dados usando o protocolo de blocos Non-Volatile Memory Express (NVMe) e Internet Small Computer Systems Interface (iSCSI). Para obter mais informações, consulte Acessando seus dados FSx do ONTAP.

Gerenciamento de FSx recursos do ONTAP

Há várias maneiras de interagir com o sistema de arquivos do ONTAP e gerenciar seus recursos. FSx Você pode gerenciar seus recursos do FSx For ONTAP usando as AWS ferramentas de gerenciamento do NetApp ONTAP:

- AWS ferramentas de gerenciamento
  - O AWS Management Console
  - O AWS Command Line Interface (AWS CLI)
  - A FSx API da Amazon e SDKs
  - AWS CloudFormation
- NetApp ferramentas de gerenciamento:
  - NetApp BlueXP
  - O NetApp ONTAP CLI
  - A API NetApp REST ONTAP

Para obter mais informações, consulte Administração de recursos.

Começando a usar a Amazon FSx para NetApp ONTAP

Saiba como começar a usar a Amazon FSx para NetApp ONTAP. Este exercício sobre os conceitos básicos inclui as etapas apresentadas a seguir.

1. Inscreva-se Conta da AWS e crie um usuário administrativo na conta.
2. Crie um sistema de arquivos Amazon FSx for NetApp ONTAP usando o FSx console da Amazon.
3. Monte seu sistema de arquivos a partir de uma instância Amazon EC2 Linux.
4. Limpe os recursos que você criou.

Tópicos

- Configurando o FSx ONTAP
- Crie um sistema de arquivos Amazon FSx for NetApp ONTAP
- Montando seu sistema de arquivos a partir de uma instância Amazon EC2 Linux
- Limpar os recursos

Configurando o FSx ONTAP

Antes de usar a Amazon FSx pela primeira vez, conclua as seguintes tarefas:

1. Inscreva-se para um Conta da AWS
2. Criar um usuário com acesso administrativo

Tópicos

- Inscreva-se para um Conta da AWS
- Criar um usuário com acesso administrativo
- Próxima etapa

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

Para obter instruções, consulte Habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

Próxima etapa

Para começar a usar o FSx ONTAP, consulte as instruções Começando a usar a Amazon FSx para NetApp ONTAP para criar seus FSx recursos da Amazon.

Crie um sistema de arquivos Amazon FSx for NetApp ONTAP

O FSx console da Amazon tem duas opções para criar um sistema de arquivos — uma opção de criação rápida e uma opção de criação padrão. Para criar de forma rápida e fácil um sistema de

arquivos Amazon FSx for NetApp ONTAP com a configuração recomendada do serviço, use a opção de criação rápida.

A opção Criação rápida configura esse sistema de arquivos para permitir o acesso a dados das instâncias do Linux pelo protocolo Network File System (NFS). Depois que seu sistema de arquivos for criado, você poderá criar volumes adicionais SVMs conforme necessário, incluindo uma SVM associada a um Active Directory para permitir o acesso de clientes Windows e macOS pelo protocolo Server Message Block (SMB). Você também pode adicionar mais pares de alta disponibilidade (HA), dependendo do tipo de implantação escolhido e de quantos pares de HA foram adicionados na criação.

Para obter informações sobre como usar a opção de criação padrão para criar um sistema de arquivos com uma configuração personalizada e para usar a API AWS CLI e, consulteCriar sistemas de arquivos.

Para criar seu sistema de arquivos do

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel, escolha Create file system (Criar sistema de arquivos) para iniciar o assistente de criação de sistemas de arquivos.
3. Na página Selecionar tipo de sistema de arquivos, escolha Amazon FSx for NetApp ONTAP e, em seguida, escolha Avançar. A página Criar sistema de arquivos ONTAP é exibida.
4. Para Método de criação, escolha Criação rápida.
5. Na seção Configuração rápida, em Nome do sistema de arquivos: opcional, insira um nome para seu sistema de arquivos. É mais fácil encontrar e gerenciar seus sistemas de arquivos quando você define um nome para eles. Você pode usar no máximo 256 letras Unicode, espaço em branco e números, além destes caracteres especiais: + - (hífen) = . _ (sublinhado) : /
6. Em Tipo de implantação, escolha Multi-AZ ou Single-AZ.

   - Os sistemas de arquivos Multi-AZ replicam dados e oferecem suporte ao failover em várias zonas de disponibilidade dentro da mesma Região da AWS.
   - Os sistemas de arquivos single-AZ replicam os dados e oferecem failover automático em uma única zona de disponibilidade.

   Para obter mais informações, consulte Opções de disponibilidade, durabilidade e implantação.

> **Note**
>
> A última geração do sistema FSx de arquivos ONTAP que está disponível para você Região da AWS é escolhida por padrão. Você pode especificar a geração do seu sistema de arquivos (se disponível Regiões da AWS) com a opção de criação padrão. Para obter mais informações, consulte Criar sistemas de arquivos.

7. Para Capacidade de armazenamento SSD, especifique a capacidade de armazenamento do seu sistema de arquivos, em gibibytes (GiB). Digite qualquer número inteiro no intervalo de 1.024 a 1.048.576. Para obter mais informações, consulte Criar um sistema de arquivos (console).

   Você pode aumentar a capacidade de armazenamento, conforme necessário, a qualquer momento após a criação do sistema de arquivos. Para obter mais informações, consulte Como gerenciar a capacidade de armazenamento.

8. Para a capacidade de transferência, a Amazon fornece FSx automaticamente uma capacidade de transferência recomendada com base no seu armazenamento SSD. Você também pode escolher a taxa de transferência do seu sistema de arquivos (até 73.728, MBps dependendo do tipo de implantação e da quantidade de pares de HA).

9. Em Nuvem privada virtual (VPC), escolha a Amazon VPC que você deseja associar ao seu sistema de arquivos.

10. Em Eficiência do armazenamento, escolha Habilitado para ativar os recursos de eficiência do armazenamento do ONTAP (eliminação da duplicação, compressão e compactação) ou selecione Desabilitado para desativar esses recursos.

11. (Somente Multi-AZ) Intervalo de endereços IP do endpoint especifica o intervalo de endereços IP no qual são criados os endpoints para acessar o sistema de arquivos.

    Escolha uma opção de criação rápida para o intervalo de endereços IP do endpoint:

    - Intervalo de endereços IP não alocados da sua VPC — Escolha essa opção para que a Amazon FSx use os últimos 64 endereços IP do intervalo CIDR primário da VPC como o intervalo de endereços IP do endpoint para o sistema de arquivos. Observe que esse intervalo será compartilhado entre vários sistemas de arquivos se você escolher essa opção várias vezes.

> **Note**
>
> - Cada sistema de arquivos que você cria consome dois endereços IP desse intervalo, um para o cluster e outro para a primeira SVM. O primeiro e o último endereço IP também são reservados. Para cada SVM adicional, o sistema de arquivos consome outro endereço IP. Por exemplo, um sistema de arquivos que hospeda 10 SVMs usa 11 endereços IP. Sistemas de arquivos adicionais funcionam da mesma maneira. Eles consomem os dois endereços IP iniciais, mais um para cada SVM adicional. O número máximo de sistemas de arquivos usando o mesmo intervalo de endereços IP, cada um com uma única SVM, é 31.
> - Essa opção ficará desabilitada se algum dos últimos 64 endereços IP no intervalo CIDR primário de uma VPC estiver sendo usado por uma sub-rede.

- Intervalo de endereços IP flutuante fora da sua VPC — Escolha essa opção para que a Amazon FSx use um intervalo de endereços de 198,1,19,x.0/24 que ainda não seja usado por nenhum outro sistema de arquivos com a mesma VPC e tabelas de rotas.

Você também pode especificar seu próprio intervalo de endereços IP na opção Criação padrão. O intervalo de endereços IP que você escolher poderá estar dentro ou fora do intervalo de endereços IP da VPC, desde que não se sobreponha a nenhuma sub-rede e que não esteja sendo usado por outro sistema de arquivos com a mesma VPC e as mesmas tabelas de rotas. Recomendamos usar um intervalo que esteja dentro do intervalo de endereços IP da VPC.

> **Note**
>
> Certifique-se de que todas as tabelas de rotas usadas estejam associadas ao seu sistema de arquivos multi-AZ. Isso ajuda a evitar a indisponibilidade durante um failover. Para obter informações sobre como associar suas tabelas de rotas da Amazon VPC ao sistema de arquivos, consulte Atualizar sistemas de arquivos.

12. Escolha Avançar e verifique a configuração do sistema de arquivos na página Criar sistema de arquivos ONTAP. Anote quais configurações do sistema de arquivos você pode modificar após a criação do sistema de arquivos.
13. Escolha Create file system (Criar sistema de arquivos).

A Criação rápida cria um sistema de arquivos com uma SVM (chamada `fsx`) e um volume (chamado `vol1`). O volume tem um caminho de junção `/vol1` e uma política de camadas do grupo de capacidade Automática (que vinculará automaticamente todos os dados que não foram acessados por 31 dias a um armazenamento de grupo de capacidade de menor custo). A política de snapshot padrão é atribuída ao volume padrão. Os dados do sistema de arquivos são criptografados em repouso usando sua AWS KMS chave gerenciada de serviço padrão.

Montando seu sistema de arquivos a partir de uma instância Amazon EC2 Linux

Você pode montar seu sistema de arquivos a partir de uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Esse procedimento usa uma instância que está executando o Amazon Linux 2.

Para montar seu sistema de arquivos da Amazon EC2

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. Crie ou selecione uma EC2 instância da Amazon executando o Amazon Linux 2 que esteja na mesma nuvem privada virtual (VPC) do seu sistema de arquivos. Para obter mais informações sobre o lançamento de uma instância, consulte Etapa 1: Executar uma instância no Guia EC2 do usuário da Amazon.
3. Conecte-se à sua instância Amazon EC2 Linux. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
4. Abra um terminal na sua EC2 instância da Amazon usando o secure shell (SSH) e faça login com as credenciais apropriadas.
5. Crie um diretório na sua EC2 instância da Amazon para usar como ponto de montagem do volume com o comando a seguir. No exemplo a seguir, *`mount-point`* substitua por suas próprias informações.

   ```
   $ sudo mkdir /mount-point
   ```

6. Monte seu sistema de arquivos Amazon FSx for NetApp ONTAP no diretório que você criou. Execute um comando `mount` semelhante ao seguinte exemplo: No exemplo a seguir, substitua os valores dos espaços reservados por suas próprias informações.

   - *`nfs_version`*— A versão do NFS que você está usando; FSx pois o ONTAP suporta as versões 3, 4.0, 4.1 e 4.2.

- *nfs-dns-name*: o nome DNS do NFS da máquina virtual de armazenamento (SVM) na qual o volume que você está montando existe. Você pode encontrar o nome DNS do NFS no FSx console da Amazon escolhendo Máquinas virtuais de armazenamento e, em seguida, escolhendo a SVM na qual o volume que você está montando existe. O nome DNS do NFS está disponível no painel Endpoints.
- *volume-junction-path*: o caminho de junção do volume que você está montando. Você pode encontrar o caminho de junção de um volume no FSx console da Amazon no painel Resumo da página de detalhes do volume.
- *mount-point*— O nome do diretório que você criou na sua EC2 instância para o ponto de montagem do volume.

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

O comando a seguir usa exemplo de valores.

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

Se você tiver problemas com sua EC2 instância da Amazon (como o tempo limite de conexões), consulte Solucionar problemas de EC2 instâncias no Guia do EC2 usuário da Amazon.

Limpar os recursos

Após concluir este exercício, siga estas etapas para limpar os recursos e proteger sua Conta da AWS.

Como limpar recursos

1. No EC2 console da Amazon, encerre sua instância. Para obter mais informações, consulte Encerre sua instância no Guia do EC2 usuário da Amazon.
2. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
3. No FSx console da Amazon, exclua todos os seus FSx volumes do ONTAP que não sejam volumes raiz do seu SVM. Para obter mais informações, consulte Excluir volumes do .

4. Exclua todos os seus FSx do ONTAP. SVMs Para obter mais informações, consulte Excluir máquinas virtuais de armazenamento (SVM).
5. No FSx console da Amazon, exclua seu sistema de arquivos. Quando você exclui um sistema de arquivos, todos os backups automáticos são excluídos automaticamente. No entanto, você ainda precisa excluir os backups criados manualmente. As seguintes etapas resumem o processo:

   a. No painel do console, escolha o nome do sistema de arquivos que você criou para este exercício.
   b. Para Ações, escolha Excluir sistema de arquivos.
   c. Na caixa de diálogo Excluir sistema de arquivos, digite o ID do sistema de arquivos que você deseja excluir, na caixa ID do sistema de arquivos.
   d. Escolha Excluir sistema de arquivos.
   e. Enquanto a Amazon FSx exclui o sistema de arquivos, seu status no painel muda para EXCLUINDO. Uma vez excluído, o sistema de arquivos não é exibido mais no painel. Todos os backups automáticos são excluídos com o sistema de arquivos.
   f. Agora você pode excluir todos os backups criados manualmente para o sistema de arquivos. No painel de navegação esquerdo, escolha Backups.
   g. No painel, escolha os backups que têm o mesmo ID de sistema de arquivos do sistema de arquivos que você excluiu e escolha Excluir backup. Certifique-se de manter o backup final, caso tenha criado um.
   h. A caixa de diálogo Excluir backups é aberta. Mantenha a caixa IDs de seleção marcada para os backups que você deseja excluir e escolha Excluir backups.

   Seu sistema de FSx arquivos da Amazon e todos os backups automáticos relacionados agora são excluídos, junto com todos os backups manuais que você optou por excluir.

Disponibilidade por Região da AWS

Os sistemas de arquivos Amazon FSx for NetApp ONTAP estão disponíveis da seguinte forma Regiões da AWS, com suporte ao tipo de implantação indicado para cada região:

Região da AWS	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
Leste dos EUA (Norte da Virgínia)	✓	✓	✓	✓		
Leste dos EUA (Ohio)	✓	✓	✓	✓		
Oeste dos EUA (Norte da Califórnia)	✓	✓	✓	✓		
Oeste dos EUA (Oregon)	✓	✓	✓	✓		
AWS GovCloud (Leste dos EUA)	✓	✓				
AWS GovCloud (Oeste dos EUA)	✓	✓				
Africa (Cape Town)	✓	✓				

Região da AWS	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
Ásia Pacífico (Hong Kong)	✓	✓				
Ásia-Pacífico (Tóquio)	✓	✓	✓	✓		
Ásia-Pacífico (Seul)	✓	✓				
Asia Pacific (Osaka)	✓	✓				
Ásia-Pacífico (Mumbai)	✓	✓	✓	✓		
Ásia-Pacífico (Hyderabad)	✓	✓				
Ásia-Pacífico (Singapura)	✓	✓	✓	✓		
Ásia-Pacífico (Sydney)	✓	✓	✓	✓		

Região da AWS	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
Ásia-Pacífico (Jacarta)	✓	✓				
Ásia-Pacífico (Melbourne)	✓	✓				
Ásia-Pacífico (Malásia)	✓	✓				
Ásia-Pacífico (Tailândia)	✓	✓				
Canadá (Central)	✓	✓				
Oeste do Canadá (Calgary)	✓	✓				
Europa (Frankfurt)	✓	✓	✓	✓		
Europa (Zurique)	✓	✓				
Europa (Estocolmo)	✓	✓	✓	✓		
Europa (Milão)	✓	✓				

Região da AWS	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
Europa (Espanha)	✓	✓				
Europa (Irlanda)	✓	✓	✓	✓		
Europa (Londres)	✓	✓				
Europa (Paris)	✓	✓				
Israel (Tel Aviv)	✓	✓				
México (Central)	✓	✓				
Oriente Médio (Emirados Árabes Unidos)	✓	✓				
Middle East (Bahrain)	✓	✓				
South America (São Paulo)	✓	✓				

Acessando seus dados FSx do ONTAP

Você pode acessar seus sistemas de FSx arquivos da Amazon usando uma variedade de clientes e métodos compatíveis nos ambientes locais Nuvem AWS e no local.

Cada SVM tem quatro endpoints que são usados para acessar dados ou gerenciar o SVM usando a NetApp CLI do ONTAP ou a API REST:

- `Nfs`: para se conectar usando o protocolo Network File System (NFS)
- `Smb`: para se conectar usando o protocolo Service Message Block (SMB) (se a SVM estiver associada a um Active Directory ou se estiver usando um grupo de trabalho).
- `Iscsi`: para se conectar usando o protocolo Internet Small Computer Systems Interface (iSCSI) para compatibilidade com armazenamento compartilhado de blocos.
- `Nvme`— Para conexão usando o Non-Volatile Memory Express (NVMe) TCP/IP para suporte ao armazenamento em blocos compartilhados.
- `Management`— Para gerenciar SVMs usando a CLI ou API NetApp ONTAP, ou BlueXP NetApp

> **Note**
>
> O protocolo iSCSI está disponível em todos os sistemas de arquivos com até 6 pares de alta disponibilidade (HA). O NVMe/TCP protocolo está disponível em sistemas de arquivos de segunda geração que têm 6 ou menos pares de HA.

Tópicos

- Clientes compatíveis
- Usar protocolos de armazenamento em bloco
- Acessando dados de dentro do Nuvem AWS
- Acesso a dados de sistemas on-premises
- Configurar o roteamento para acessar sistemas de arquivos Multi-AZ de fora de sua VPC
- Configurar o roteamento para acessar sistemas de arquivos Multi-AZ on-premises
- Montagem de volumes em clientes Linux
- Montar volumes em clientes Microsoft Windows
- Montagem de volumes em clientes macOS

- Provisionamento de iSCSI para Linux
- Provisionamento de iSCSI para Windows
- Provisionamento NVMe /TCP para Linux
- Provisionamento para Windows NVMe/TCP
- Acessar dados com outros serviços da AWS

Clientes compatíveis

FSx Os sistemas de arquivos for ONTAP oferecem suporte ao acesso a dados de uma ampla variedade de instâncias computacionais e sistemas operacionais. Isso é feito oferecendo suporte ao acesso com o protocolo Network File System (NFS) (v3, v4.0, v4.1 e v4.2), todas as versões do protocolo Server Message Block (SMB) (incluindo 2.0, 3.0 e 3.1.1) e o protocolo Internet Small Computer Systems Interface (iSCSI).

> **Important**
>
> A Amazon FSx não oferece suporte ao acesso a sistemas de arquivos da Internet pública. A Amazon separa FSx automaticamente qualquer endereço IP elástico, que é um endereço IP público acessível pela Internet, que é anexado à interface de rede elástica de um sistema de arquivos.

As seguintes instâncias AWS de computação são compatíveis para uso com o FSx ONTAP:

- Instâncias do Amazon Elastic Compute Cloud (Amazon EC2) executando Linux com suporte a NFS ou SMB, Microsoft Windows e macOS. Para obter mais informações, consulte Montagem de volumes em clientes Linux, Montar volumes em clientes Microsoft Windows e Montagem de volumes em clientes macOS.
- Contêineres Docker do Amazon Elastic Container Service (Amazon ECS) em instâncias do EC2 Amazon Windows e Linux. Para obter mais informações, consulte Usando o Amazon Elastic Container Service com FSx o ONTAP.
- Amazon Elastic Kubernetes Service — Para saber mais, consulte o driver CSI Amazon NetApp for ONTAP no Guia do usuário do FSx Amazon EKS.
- Red Hat OpenShift Service on AWS (ROSA) — Para saber mais, consulte What is Red Hat OpenShift Service on AWS? no Guia do AWS Usuário do Red Hat OpenShift Service on.

- WorkSpaces Instâncias da Amazon. Para obter mais informações, consulte Usando a Amazon WorkSpaces com o FSx ONTAP.
- Instâncias da Amazon AppStream 2.0.
- AWS Lambda — Para obter mais informações, consulte a postagem do AWS blog Habilitando o acesso de pequenas e médias empresas para cargas de trabalho sem servidor com a Amazon. FSx
- Máquinas virtuais (VMs) em execução na VMware nuvem em AWS ambientes. Para obter mais informações, consulte Configurar o Amazon FSx para NetApp ONTAP como armazenamento externo e VMware Cloud on AWS with Amazon FSx for NetApp ONTAP Deployment Guide.

Uma vez montados, FSx os sistemas de arquivos ONTAP aparecem como um diretório local ou letra de drive em NFS e SMB, fornecendo armazenamento de arquivos em rede totalmente gerenciado e compartilhado que pode ser acessado simultaneamente por até milhares de clientes. Os LUNS iSCSI são acessíveis como dispositivos de bloco quando montados em iSCSI.

Usar protocolos de armazenamento em bloco

O Amazon FSx for NetApp ONTAP oferece suporte à Internet Small Computer Systems Interface (iSCSI) e à Non-Volatile Memory Express NVMe () via TCP NVMe/TCP) block storage protocols. In Storage Area Network (SAN) environments, storage systems are targets that have storage target devices. For iSCSI, the storage target devices are referred to as logical units (LUNs). For NVMe/TCP (), os dispositivos de destino de armazenamento são chamados de namespaces.

Você usa a interface lógica iSCSI (LIF) de um SVM para se conectar a ambos NVMe e ao armazenamento em blocos iSCSI.

Você configura o armazenamento criando LUNs para iSCSI e criando namespaces para. NVMe LUNs e os namespaces são então acessados pelos hosts usando os protocolos iSCSI ou TCP.

Para obter mais informações sobre como configurar iSCSI NVMe/TCP e armazenamento em blocos, consulte:

- Provisionamento de iSCSI para Linux
- Provisionamento de iSCSI para Windows
- Provisionamento NVMe /TCP para Linux
- Provisionamento para Windows NVMe/TCP

> **Note**
>
> O provisionamento NVMe/TCP para Windows requer o uso de um iniciador NVMe terceirizado.

Acessando dados de dentro do Nuvem AWS

Cada sistema de FSx arquivos da Amazon está associado a uma Virtual Private Cloud (VPC). Você pode acessar seu sistema de arquivos FSx for ONTAP de qualquer lugar na VPC do sistema de arquivos, independentemente da zona de disponibilidade. Você também pode acessar seu sistema de arquivos de outros VPCs que podem estar em AWS contas diferentes ou Regiões da AWS. Além dos requisitos descritos nas seções a seguir FSx para acessar os recursos do ONTAP, você também precisa garantir que o grupo de segurança VPC do seu sistema de arquivos esteja configurado para que o tráfego de dados e gerenciamento possa fluir entre o sistema de arquivos e os clientes. Para obter mais informações sobre a configuração de grupos de segurança com as portas necessárias, consulte Grupos de segurança da Amazon VPC.

Acesso a dados de dentro da mesma VPC

Ao criar seu sistema de arquivos Amazon FSx for NetApp ONTAP, você seleciona a Amazon VPC na qual ele está localizado. Todos SVMs os volumes associados ao sistema de arquivos Amazon FSx for NetApp ONTAP também estão localizados na mesma VPC. Ao montar um volume, se o sistema de arquivos e o cliente que monta o volume estiverem localizados na mesma VPC Conta da AWS, você poderá usar o nome DNS e a junção de volume ou o compartilhamento SMB do SVM, dependendo do cliente.

Você pode obter uma performance ideal se o cliente e o volume estiverem localizados na mesma zona de disponibilidade da sub-rede do sistema de arquivos ou na sub-rede preferencial dos sistemas de arquivos multi-AZ. Para identificar a sub-rede ou sub-rede preferencial de um sistema de arquivos, no FSx console da Amazon, escolha Sistemas de arquivos e, em seguida, escolha o sistema de arquivos ONTAP cujo volume você está montando, e a sub-rede ou sub-rede preferencial (Multi-AZ) é exibida no painel Sub-rede ou Sub-rede preferencial.

Acesso a dados de fora da VPC de implantação

Esta seção descreve como acessar os endpoints do sistema de arquivos FSx for ONTAP de AWS locais fora da VPC de implantação do sistema de arquivos.

Acesso a endpoints NFS, SMB e de gerenciamento do ONTAP em sistemas de arquivos multi-AZ

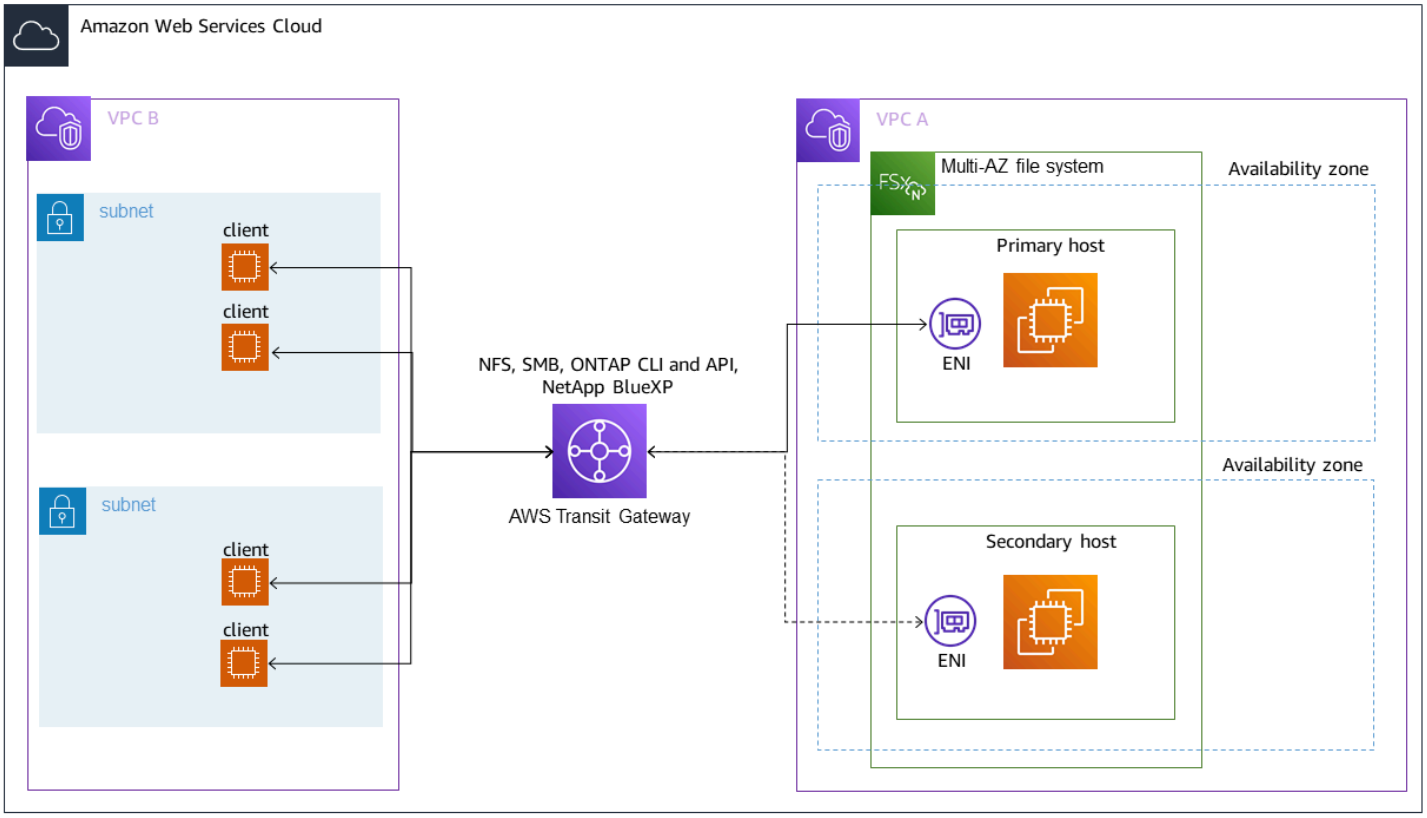
Os endpoints de gerenciamento NFS, SMB e ONTAP na FSx Amazon NetApp para sistemas de arquivos ONTAP Multi-AZ usam endereços de protocolo de internet (IP) flutuantes para que os clientes conectados façam uma transição perfeita entre os servidores de arquivos preferenciais e os de espera durante um evento de failover. Para obter mais informações sobre failovers, consulte Processo de failover FSx para ONTAP.

Esses endereços IP flutuantes são criados nas tabelas de rotas da VPC associadas ao sistema de arquivos, estando dentro do `EndpointIpAddressRange` do sistema de arquivos que você pode especificar durante a criação. O `EndpointIpAddressRange` usa os intervalos de endereços a seguir, dependendo de como um sistema de arquivos é criado.

- Os sistemas de arquivos Multi-AZ criados usando o FSx console da Amazon usam, por padrão, os últimos 64 endereços IP no intervalo CIDR primário da VPC para o sistema de `EndpointIpAddressRange` arquivos.
- Os sistemas de arquivos Multi-AZ criados usando a FSx API AWS CLI ou a Amazon usam um intervalo de endereços IP dentro do bloco de `198.19.0.0/16` endereços para o, `EndpointIpAddressRange` por padrão.
- Você também pode especificar seu próprio intervalo de endereços IP ao usar a opção de criação padrão. O intervalo de endereços IP que você escolher poderá estar dentro ou fora do intervalo de endereços IP da VPC, desde que não se sobreponha a nenhuma sub-rede e que não esteja sendo usado por outro sistema de arquivos com a mesma VPC e as mesmas tabelas de rotas. Para essa opção, recomendamos usar um intervalo que esteja dentro do intervalo de endereços IP da VPC.

Somente AWS Transit Gateway oferece suporte ao roteamento para endereços IP flutuantes, também conhecido como emparelhamento transitivo. Peering de VPC, AWS Direct Connect, e AWS VPN não oferecem suporte ao peering transitivo. Portanto, é necessário usar o Transit Gateway para acessar essas interfaces de redes que estão fora da VPC do sistema de arquivos.

O diagrama a seguir ilustra o uso do Transit Gateway para NFS, SMB ou acesso de gerenciamento a um sistema de arquivos multi-AZ que está em uma VPC diferente da dos clientes que o estão acessando.



> **Note**
>
> Certifique-se de que todas as tabelas de rotas usadas estejam associadas ao seu sistema de arquivos multi-AZ. Isso ajuda a evitar a indisponibilidade durante um failover. Para obter informações sobre como associar suas tabelas de rotas da Amazon VPC ao sistema de arquivos, consulte Atualizar sistemas de arquivos.

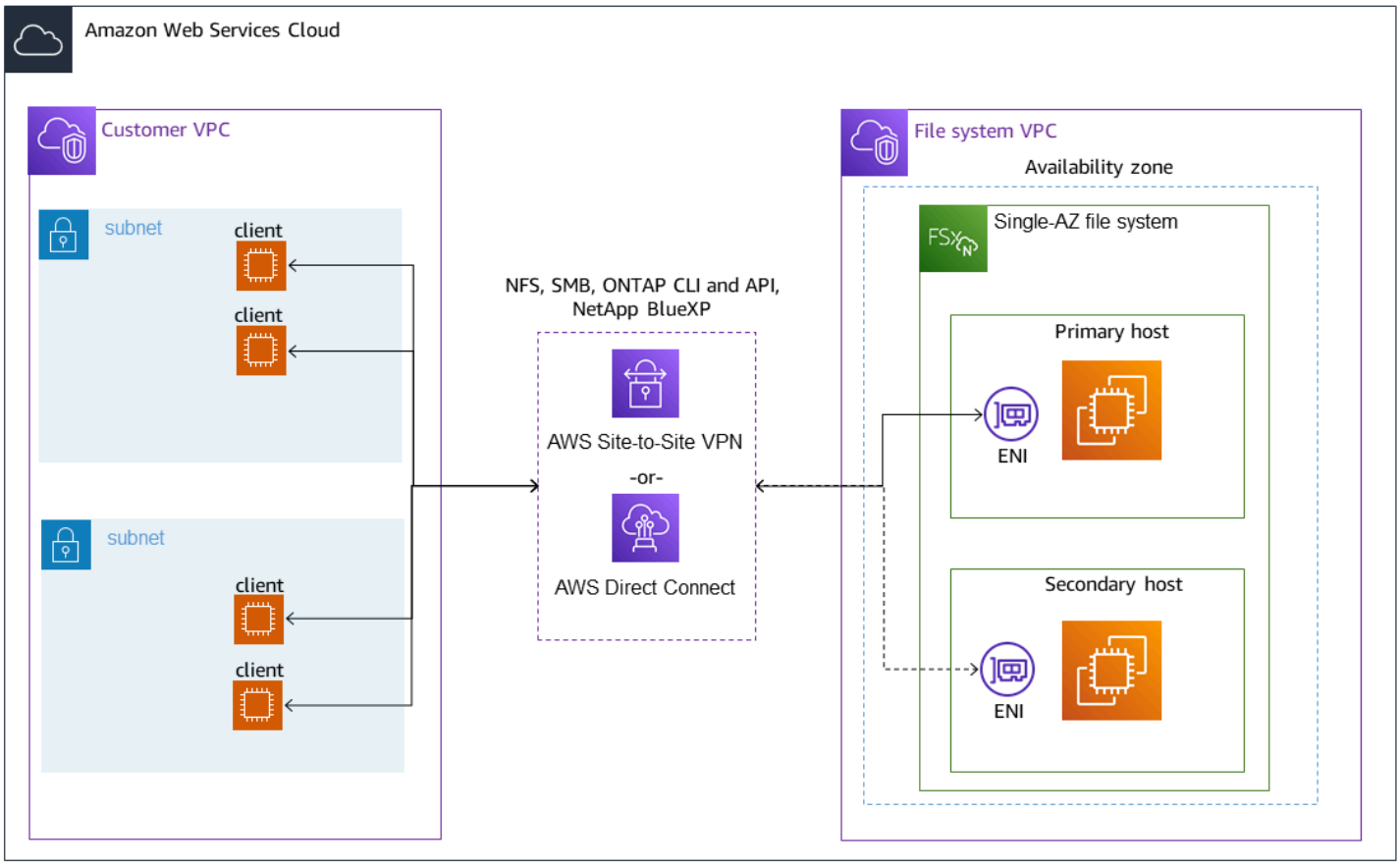
Para obter informações sobre quando você precisa usar o Transit Gateway para acessar seu sistema de arquivos FSx para ONTAP, consulteQuando o Transit Gateway é necessário?.

A Amazon FSx gerencia tabelas de rotas de VPC para sistemas de arquivos Multi-AZ usando autenticação baseada em tags. Essas tabelas de rotas serão marcadas com `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Ao criar ou atualizar FSx para sistemas de arquivos ONTAP Multi-AZ usando, AWS CloudFormation recomendamos que você adicione a `Key: AmazonFSx; Value: ManagedByAmazonFSx` tag manualmente.

Acesso a NFS, SMB ou a CLI e API do ONTAP para sistemas de arquivos single-AZ

Os endpoints usados FSx para acessar os sistemas de arquivos ONTAP Single-AZ via NFS ou SMB e para administrar sistemas de arquivos usando a CLI do ONTAP ou a API REST são endereços IP secundários na ENI do servidor de arquivos ativo. Os endereços IP secundários estão dentro do intervalo CIDR da VPC, então os clientes podem acessar dados e portas de gerenciamento usando o VPC Peering ou sem necessidade. AWS Direct Connect AWS VPN AWS Transit Gateway

O diagrama a seguir ilustra como usar AWS VPN ou AWS Direct Connect para NFS, SMB ou acesso de gerenciamento a um sistema de arquivos Single-AZ que está em uma VPC diferente da dos clientes que o acessam.



Quando o Transit Gateway é necessário?

Se o Transit Gateway é necessário ou não para os sistemas de arquivos multi-AZ depende do método usado para acessar os dados do sistema de arquivos. Os sistemas de arquivos single-AZ não exigem o Transit Gateway. A tabela a seguir descreve quando você precisará usar o AWS Transit Gateway para acessar sistemas de arquivos multi-AZ.

Acesso aos dados	Requer o Transit Gateway?
FSx Acessando via NFS, SMB ou NetApp ONTAP REST API, CLI ou BlueXP	Somente se: • Acessar de uma rede emparelhada (on-premises, por exemplo) e • Você não está acessando FSx por meio de uma NetApp FlexCache instância do Global File Cache
Acessar dados por meio de iSCSI	Não
Acessando dados por NVMe	Não
Associar uma SVM a um Active Directory	Não
SnapMirror	Não
FlexCache Armazenamento em cache	Não
Global File Cache	Não

Acesso NVMe a endpoints iSCSI e entre clusters fora da VPC de implantação

Você pode usar o VPC Peering ou AWS Transit Gateway acessar o sistema de arquivos, NVMe iSCSI e endpoints entre clusters de fora da VPC de implantação do sistema de arquivos. Você pode usar o VPC Peering para rotear, NVMe iSCSI e tráfego entre clusters. VPCs Uma conexão de emparelhamento VPC é uma conexão de rede entre duas VPCs e é usada para rotear o tráfego entre elas usando endereços privados. IPv4 Você pode usar o emparelhamento de VPC para se conectar VPCs dentro da mesma Região da AWS ou entre diferentes. Regiões da AWS Para obter mais informações sobre o emparelhamento da VPC, consulte O que é emparelhamento de VPC? no Guia de emparelhamento da Amazon VPC.

Acesso a dados de sistemas on-premises

Você pode acessar seus sistemas de arquivos FSx for ONTAP no local usando AWS VPNe. AWS Direct Connectdiretrizes de casos de uso mais específicas estão disponíveis nas seções a seguir. Além dos requisitos listados abaixo para acessar diferentes FSx recursos do ONTAP no local,

você também precisa garantir que o grupo de segurança VPC do seu sistema de arquivos permita que os dados fluam entre seu sistema de arquivos e os clientes; para obter uma lista das portas necessárias, consulte Grupos de segurança do Amazon VPC.

Acessar endpoints NFS, SMB ou da CLI ou API REST do ONTAP de sistemas on-premises

Esta seção descreve como acessar as portas de gerenciamento NFS, SMB e ONTAP nos sistemas de arquivos ONTAP FSx a partir de redes locais.

Acessar sistemas de arquivos Multi-AZ on-premises

A Amazon FSx exige que você use AWS Transit Gateway ou configure o NetApp Global File Cache remoto ou acesse sistemas NetApp FlexCache de arquivos Multi-AZ a partir de uma rede local. Para oferecer suporte ao failover em zonas de disponibilidade para sistemas de arquivos Multi-AZ, a Amazon FSx usa endereços IP flutuantes para as interfaces usadas para endpoints de gerenciamento NFS, SMB e ONTAP.

Como os endpoints NFS, SMB e de gerenciamento usam endereços IP flutuantes, você deve usar AWS Transit Gatewayem conjunto com AWS Direct Connect ou AWS VPN para acessar essas interfaces a partir de uma rede local. Os endereços IP flutuantes usados nessas interfaces estão dentro do `EndpointIpAddressRange` que você especifica ao criar o sistema de arquivos multi-AZ. O `EndpointIpAddressRange` usa os intervalos de endereços a seguir, dependendo de como um sistema de arquivos é criado.

- Os sistemas de arquivos Multi-AZ criados usando o FSx console da Amazon usam, por padrão, os últimos 64 endereços IP no intervalo CIDR primário da VPC para o sistema de `EndpointIpAddressRange` arquivos.
- Os sistemas de arquivos Multi-AZ criados usando a FSx API AWS CLI ou a Amazon usam um intervalo de endereços IP dentro do bloco de `198.19.0.0/16` endereços para o, `EndpointIpAddressRange` por padrão.
- Você também pode especificar seu próprio intervalo de endereços IP ao usar a opção de criação padrão no FSx console da Amazon. O intervalo de endereços IP escolhido pode estar dentro ou fora do intervalo de endereços IP da VPC, desde que não se sobreponha a nenhuma sub-rede e desde que ainda não seja usado por outro sistema de arquivos com a mesma VPC e tabelas de rotas. Para essa opção, recomendamos usar um intervalo que esteja dentro do intervalo de endereços IP da VPC.

Os endereços IP flutuantes são usados para permitir uma transição sem interrupções dos clientes para o sistema de arquivos em espera, caso seja necessário um failover. Para obter mais informações, consulte Processo de failover FSx para ONTAP.

> **Important**
>
> Para acessar um sistema de arquivos multi-AZ usando um Transit Gateway, cada um dos anexos do Transit Gateway deve ser criado em uma sub-rede cuja tabela de rotas esteja associada ao sistema de arquivos.

Para obter mais informações, consulte Configurar o roteamento para acessar sistemas de arquivos Multi-AZ on-premises.

Acessando sistemas de arquivos Single-AZ localmente

O requisito de uso AWS Transit Gateway para acessar dados de uma rede local não existe para sistemas de arquivos Single-AZ. Os sistemas de arquivos single-AZ são implantados em uma única sub-rede, e um endereço IP flutuante não é necessário para fornecer failover entre os nós. Em vez disso, os endereços IP que você acessa nos sistemas de arquivos single-AZ são implementados como endereços IP secundários dentro do intervalo CIDR da VPC do sistema de arquivos, permitindo que você acesse seus dados de outra rede sem precisar do AWS Transit Gateway.

Acesso a endpoints entre clusters de sistemas on-premises

FSx os endpoints entre clusters do ONTAP são dedicados ao tráfego de replicação entre os sistemas de arquivos NetApp ONTAP, inclusive entre implantações locais NetApp e para o ONTAP. FSx O tráfego de replicação inclui SnapMirror, FlexCache, e FlexClone relacionamentos entre máquinas virtuais de armazenamento (SVMs) e volumes em diferentes sistemas de arquivos e o NetApp Global File Cache. Os endpoints entre clusters também são usados para o tráfego do Active Directory.

Como os endpoints entre clusters de um sistema de arquivos usam endereços IP que estão dentro do intervalo CIDR da VPC que você fornece ao criar seu sistema de arquivos FSx para ONTAP, você não precisa usar um Transit Gateway para rotear o tráfego entre clusters entre o local e o. Nuvem AWS No entanto, os clientes locais ainda precisam usar AWS VPN ou AWS Direct Connect estabelecer uma conexão segura com sua VPC.

Para obter mais informações, consulte Configurar o roteamento para acessar sistemas de arquivos Multi-AZ on-premises.

Configurar o roteamento para acessar sistemas de arquivos Multi-AZ de fora de sua VPC

Se você tiver um sistema de arquivos Multi-AZ com um `EndpointIPAddressRange` que esteja fora do intervalo de endereços IP da sua VPC, precisará configurar um roteamento adicional para acessar seu sistema de arquivos AWS Transit Gateway a partir de redes locais ou com peering.

Important

Para acessar um sistema de arquivos multi-AZ usando um Transit Gateway, cada um dos anexos do Transit Gateway deve ser criado em uma sub-rede cuja tabela de rotas esteja associada ao sistema de arquivos.

Note

Nenhuma configuração adicional do Transit Gateway é necessária para sistemas de arquivos single-AZ ou sistemas de arquivos multi-AZ com um `EndpointIPAddressRange` que esteja dentro da faixa de endereços IP da sua VPC.

Para configurar o roteamento usando AWS Transit Gateway

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Escolha o FSx sistema de arquivos ONTAP para o qual você está configurando o acesso de uma rede com peering.
3. Em Rede e segurança, copie o Intervalo de endereços IP do endpoint.
4. Adicione uma rota ao Transit Gateway que roteie o tráfego destinado a esse intervalo de endereços IP para a VPC do sistema de arquivos. Para obter mais informações, consulte Trabalhar com gateways de trânsito em Gateways de trânsito da Amazon VPC.
5. Confirme se você pode acessar seu sistema de arquivos FSx for ONTAP a partir da rede com peering.

Para adicionar a tabela de rotas ao sistema de arquivos, consulte Atualizar sistemas de arquivos.

> **Note**
>
> Os registros DNS dos endpoints de gerenciamento, NFS e SMB só podem ser resolvidos na mesma VPC do sistema de arquivos. Para montar um volume ou conectar-se a uma porta de gerenciamento de outra rede, é necessário usar o endereço IP do endpoint. Esses endereços IP não mudam com o tempo.

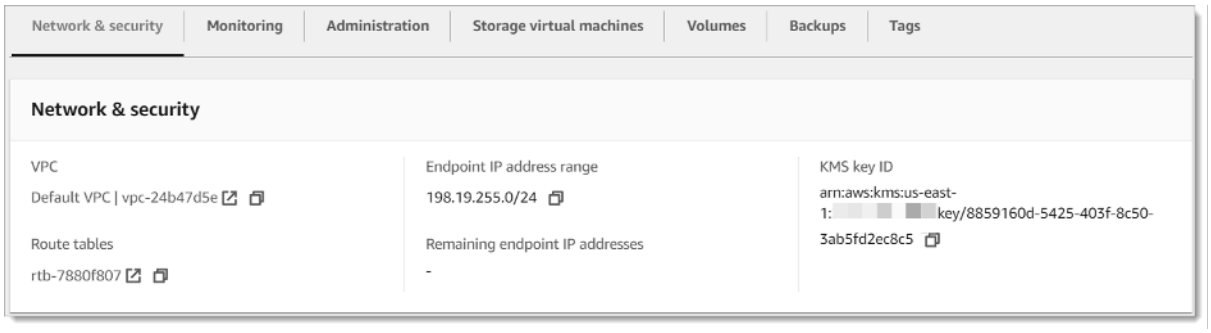
Configurar o roteamento para acessar sistemas de arquivos Multi-AZ on-premises

AWS Transit Gateway Para configurar o acesso aos sistemas de arquivos Multi-AZ a partir do local

Se você tiver um sistema de arquivos Multi-AZ com um `EndpointIPAddressRange` que esteja fora do intervalo CIDR da sua VPC, precisará configurar um roteamento adicional para acessar seu sistema de arquivos AWS Transit Gateway a partir de redes locais ou com peering.

> **Note**
>
> Nenhuma configuração adicional do Transit Gateway é necessária para sistemas de arquivos single-AZ ou sistemas de arquivos multi-AZ com um `EndpointIPAddressRange` que esteja dentro da faixa de endereços IP da sua VPC.

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Escolha o FSx sistema de arquivos ONTAP para o qual você está configurando o acesso de uma rede com peering.
3. Em Rede e segurança, copie o Intervalo de endereços IP do endpoint.



4. Adicione uma rota ao Transit Gateway que roteie o tráfego destinado a esse intervalo de endereços IP para a VPC do seu sistema de arquivos. Para obter mais informações, consulte Trabalhar com gateways de trânsito no Guia do usuário do Amazon VPC Transit Gateway.
5. Confirme se você pode acessar seu sistema de arquivos FSx for ONTAP a partir da rede com peering.

> **Important**
>
> Para acessar um sistema de arquivos multi-AZ usando um Transit Gateway, cada um dos anexos do Transit Gateway deve ser criado em uma sub-rede cuja tabela de rotas esteja associada ao sistema de arquivos. Quando você tem sub-redes anexadas separadas do Transit Gateway, você também deve associar as tabelas de rotas dessas sub-redes à FSx Amazon para que elas sejam atualizadas com os endereços de endpoint da Amazon FSx .

Para adicionar uma tabela de rotas ao sistema de arquivos, consulte Atualizar sistemas de arquivos.

Montagem de volumes em clientes Linux

Recomendamos que os volumes que deseja montar com clientes Linux tenham uma configuração de estilo de segurança de `UNIX` ou `mixed`. Para obter mais informações, consulte Gerenciamento FSx de volumes ONTAP.

> **Note**
>
> Por padrão, FSx para ONTAP, montagens NFS são montagens. `hard` Para garantir um failover tranquilo caso ocorra, recomendamos que use a opção de montagem `hard` padrão.

Montar um volume do ONTAP em um cliente Linux

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. Crie ou selecione uma EC2 instância da Amazon executando o Amazon Linux 2 que esteja na mesma VPC do sistema de arquivos.

   Para obter mais informações sobre o lançamento de uma instância EC2 Linux, consulte Etapa 1: Executar uma instância no Guia EC2 do usuário da Amazon.

3. Conecte-se à sua instância Amazon EC2 Linux. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
4. Abra um terminal na sua EC2 instância usando o secure shell (SSH) e faça login com as credenciais apropriadas.
5. Crie um diretório na EC2 instância para montar o volume SVM da seguinte forma:

```
sudo mkdir /fsx
```

6. Monte o volume no diretório que acabou de criar usando o seguinte comando:

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

O exemplo a seguir usa valores de amostra.

```
sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
east-1.amazonaws.com:/vol1 /fsx
```

Você também pode usar o endereço IP da SVM em vez do nome DNS. Recomendamos usar o nome de DNS para montar clientes em sistemas de arquivos de segunda geração, pois isso ajuda a garantir que seus clientes sejam balanceados entre os pares de alta disponibilidade (HA) do sistema de arquivos.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

> **Note**
>
> Para sistemas de arquivos de segunda geração, o protocolo NFS paralelo (pNFS) é habilitado por padrão e usado por padrão para qualquer cliente que monte volumes com NFS v4.1 ou superior.

Como usar /etc/fstab para montar automaticamente na reinicialização da instância

Para remontar automaticamente seu volume FSx para ONTAP quando uma instância do Amazon EC2 Linux for reinicializada, use o arquivo. `/etc/fstab` O arquivo `/etc/fstab` contém

informações sobre sistemas de arquivos. O comando `mount -a`, que é executado durante a inicialização da instância, monta os sistemas de arquivos listados em `/etc/fstab`.

> **Note**
>
> FSx para sistemas de arquivos ONTAP, não há suporte para montagem automática `/etc/fstab` em instâncias do Amazon EC2 Mac.

> **Note**
>
> Antes de atualizar o `/etc/fstab` arquivo da sua EC2 instância, verifique se você já criou seu sistema de arquivos FSx for ONTAP. Para obter mais informações, consulte Criar sistemas de arquivos.

Para atualizar o arquivo /etc/fstab na sua instância EC2

1. Conecte-se à sua EC2 instância:

   - Para se conectar à instância em um computador com macOS ou Linux, especifique o arquivo .pem para o comando SSH. Para fazer isso, use a opção `-i` e o caminho para sua chave privada.
   - Para se conectar à sua instância a partir de um computador executando o Windows, você pode usar MindTerm ou PuTTY. Para usar o PuTTY, instale-o e converta o arquivo .pem para um arquivo .ppk.

   Para obter mais informações, consulte os seguintes tópicos no Guia do EC2 usuário da Amazon:

   - Conectar à sua instância do Linux usando SSH
   - Conectar à instância do Linux a partir do Windows usando PuTTY
2. Crie um diretório local que será usado para montar o volume da SVM.

   ```
   sudo mkdir /fsx
   ```
3. Abra o arquivo `/etc/fstab` com seu editor de preferência.

4. Adicione a linha a seguir ao arquivo `/etc/fstab`. Insira um caractere de tabulação entre cada parâmetro. Deve aparecer como uma linha sem quebras de linha.

   ```
   svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
   ```

   Também é possível usar o endereço IP da SVM do volume. Os três últimos parâmetros indicam opções de NFS (que definimos como padrão), despejo do sistema de arquivos e verificação do sistema de arquivos (normalmente não são usados, então os definimos como 0).

5. Salve a alteração no arquivo.
6. Agora, monte o compartilhamento de arquivos usando o comando a seguir. Na próxima vez em que o sistema for iniciado, a pasta será montada automaticamente.

   ```
   sudo mount /fsx
   sudo mount svm-dns-name:volume-junction-path
   ```

Sua EC2 instância agora está configurada para montar o volume ONTAP sempre que for reiniciado.

Montar volumes em clientes Microsoft Windows

Esta seção descreve como acessar dados em seu sistema de arquivos FSx para ONTAP com clientes que executam o sistema operacional Microsoft Windows. Analise os requisitos a seguir, independentemente do tipo de cliente que está usando.

Este procedimento pressupõe que o cliente e o sistema de arquivos estejam localizados na mesma VPC e Conta da AWS. Se o cliente estiver localizado no local ou em uma VPC diferente, ou Conta da AWS Região da AWS, esse procedimento também pressupõe que você tenha configurado ou uma conexão de rede dedicada usando AWS Transit Gateway AWS Direct Connect ou usando um túnel privado e seguro. AWS Virtual Private Network Para obter mais informações, consulte Acesso a dados de fora da VPC de implantação.

Recomendamos que você anexe volumes aos clientes Windows usando o protocolo SMB.

Pré-requisitos

Para acessar um volume de armazenamento do ONTAP usando um cliente Microsoft Windows, é necessário atender aos pré-requisitos a seguir.

- A SVM do volume que você está anexando deve estar associada ao Active Directory da sua organização ou você deve estar usando um grupo de trabalho. Para obter mais informações sobre como associar a SVM a um Active Directory, consulte Gerenciamento FSx de máquinas virtuais de armazenamento ONTAP. Para obter mais informações sobre o uso de grupos de trabalho, consulteConfigurando um servidor SMB em um grupo de trabalho.
- O volume que você está anexando tem uma configuração de estilo de segurança de `NTFS` ou `mixed`. Para obter mais informações, consulte Estilo de segurança do volume.

Para montar um volume em um cliente Windows usando o Active Directory e SMB

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. Crie ou selecione uma EC2 instância da Amazon executando o Microsoft Windows que esteja na mesma VPC do sistema de arquivos e associada ao mesmo Microsoft Active Directory da SVM do volume.

   Para obter mais informações sobre o lançamento de uma instância, consulte Etapa 1: Executar uma instância no Guia EC2 do usuário da Amazon.

   Para obter mais informações sobre como associar uma SVM a um Active Directory, consulte Gerenciamento FSx de máquinas virtuais de armazenamento ONTAP.
3. Conecte-se à sua instância EC2 do Amazon Windows. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia EC2 do usuário da Amazon.
4. Abra um prompt de comando.
5. Execute o seguinte comando: Substitua o seguinte:

   - Substitua `Z:` por qualquer letra de unidade disponível.
   - Substitua `DNS_NAME` pelo nome DNS ou pelo endereço IP do endpoint SMB da SVM do volume.
   - Substitua `SHARE_NAME` pelo nome de um compartilhamento SMB. `C$` é o compartilhamento SMB padrão na raiz do namespace do SVM, mas você não deve montá-lo, pois isso expõe o armazenamento ao volume raiz e pode causar interrupções na segurança e no serviço. Em vez de `C$`, você deverá fornecer um nome de compartilhamento SMB para montar. Para obter mais informações sobre como criar compartilhamentos SMB, consulte Como gerenciar compartilhamentos de SMB.

```
net use Z: \\DNS_NAME\SHARE_NAME
```

O exemplo a seguir usa valores de amostra.

```
net use Z: \\corp.example.com\group_share
```

Você também pode usar o endereço IP da SVM em vez do nome DNS. Recomendamos usar o nome de DNS para montar clientes em sistemas de arquivos de segunda geração, pois isso ajuda a garantir que seus clientes sejam balanceados entre os pares de alta disponibilidade (HA) do sistema de arquivos.

```
net use Z: \\198.51.100.5\group_share
```

Montagem de volumes em clientes macOS

Esta seção descreve como acessar dados em seu FSx sistema de arquivos do ONTAP com clientes que executam o sistema operacional macOS. Analise os requisitos a seguir, independentemente do tipo de cliente que está usando.

Este procedimento pressupõe que o cliente e o sistema de arquivos estejam localizados na mesma VPC e Conta da AWS. Se o cliente estiver localizado no local ou em uma VPC diferente Região da AWS, Conta da AWS ou se você tiver configurado uma conexão de rede dedicada usando AWS Transit Gateway AWS Direct Connect ou usando um túnel privado e seguro. AWS Virtual Private Network Para obter mais informações, consulte Acesso a dados de fora da VPC de implantação.

Recomendamos que você anexe volumes aos seus clientes Mac usando o protocolo SMB.

Montar um volume do ONTAP em um cliente macOS usando SMB

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. Crie ou selecione uma instância do Amazon EC2 Mac executando o macOS que esteja na mesma VPC do sistema de arquivos.

   Para obter mais informações sobre como iniciar uma instância, consulte Etapa 1: Executar uma instância no Guia EC2 do usuário da Amazon.

3. Conecte-se à sua instância Amazon EC2 Mac. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
4. Abra um terminal na sua EC2 instância usando o secure shell (SSH) e faça login com as credenciais apropriadas.
5. Crie um diretório na EC2 instância para montar o volume da seguinte maneira:

```
sudo mkdir /fsx
```

6. Monte o volume usando o comando a seguir.

```
sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
```

O exemplo a seguir usa valores de amostra.

```
sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-
east-1.amazonaws.com:/C$ /fsx
```

Você também pode usar o endereço IP da SVM em vez do nome DNS. Recomendamos usar o nome de DNS para montar clientes em sistemas de arquivos de segunda geração, pois isso ajuda a garantir que seus clientes sejam balanceados entre os pares de alta disponibilidade (HA) do sistema de arquivos.

```
sudo mount -t smbfs 198.51.100.10:/C$ /fsx
```

`C$` é o compartilhamento SMB padrão que você pode montar para ver a raiz do namespace da SVM. Se você criou algum compartilhamento Server Message Block (SMB) na SVM, forneça os nomes dos compartilhamentos SMB em vez de `C$`. Para obter mais informações sobre como criar compartilhamentos SMB, consulte Como gerenciar compartilhamentos de SMB.

Montar um volume do ONTAP em um cliente macOS usando NFS

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. Crie ou selecione uma EC2 instância da Amazon executando o Amazon Linux 2 que esteja na mesma VPC do sistema de arquivos.

   Para obter mais informações sobre o lançamento de uma instância EC2 Linux, consulte Etapa 1: Executar uma instância no Guia EC2 do usuário da Amazon.

3. Conecte-se à sua instância Amazon EC2 Linux. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
4. Monte seu volume FSx for ONTAP na EC2 instância Linux usando um script de dados do usuário durante a execução da instância ou executando os seguintes comandos:

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-point
```

O exemplo a seguir usa valores de amostra.

```
sudo mount -t nfs -o nfsvers=4.1
 svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
fsxontap
```

Você também pode usar o endereço IP da SVM em vez do nome DNS. Recomendamos usar o nome de DNS para montar clientes em sistemas de arquivos de segunda geração, pois isso ajuda a garantir que seus clientes sejam balanceados entre os pares de HA do sistema de arquivos.

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. Monte o volume no diretório que acabou de criar usando o comando a seguir.

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

O exemplo a seguir usa valores de amostra.

```
sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
east-1.amazonaws.com:/vol1 /fsx
```

Você também pode usar o endereço IP da SVM em vez do nome DNS. Recomendamos usar o nome de DNS para montar clientes em sistemas de arquivos de segunda geração, pois isso ajuda a garantir que seus clientes sejam balanceados entre os pares de alta disponibilidade (HA) do sistema de arquivos.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

Provisionamento de iSCSI para Linux

FSx for ONTAP suporta o protocolo iSCSI. Você precisa provisionar iSCSI no cliente Linux e no sistema de arquivos para usar o protocolo iSCSI para transportar dados entre clientes e seu sistema de arquivos. O protocolo iSCSI está disponível em todos os sistemas de arquivos com até 6 pares de alta disponibilidade (HA).

Há três etapas principais para o processo de configuração do iSCSI em seu FSx Amazon NetApp for ONTAP, que são abordadas nos seguintes procedimentos:

1. Instale e configure o cliente iSCSI no host Linux.
2. Configure o iSCSI na SVM do sistema de arquivos.
   - Crie um grupo de iniciadores iSCSI.
   - Mapeie o grupo de iniciadores para a LUN.
3. Monte uma LUN iSCSI no cliente Linux,

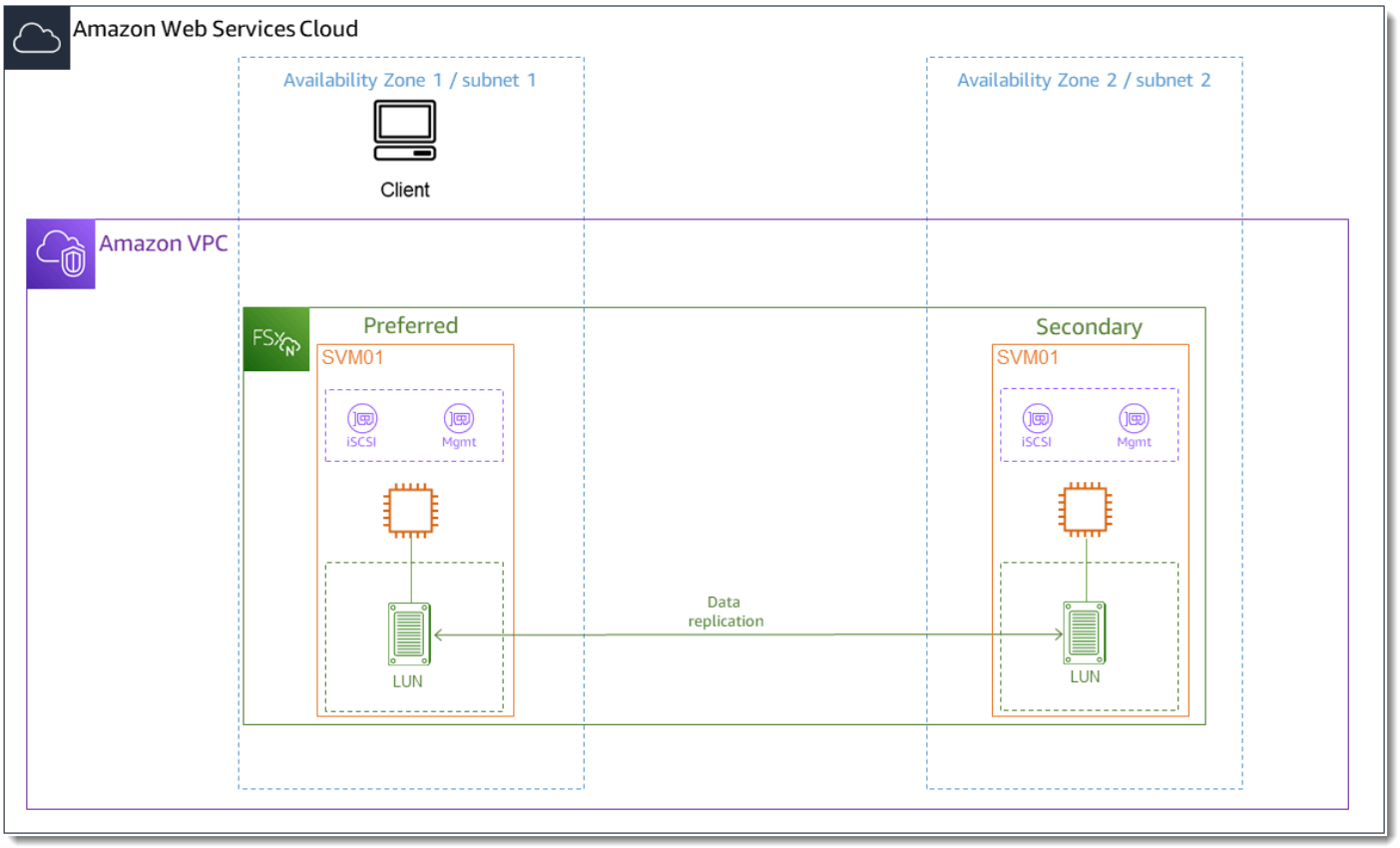
Antes de começar

Antes de iniciar o processo de configuração do sistema de arquivos para iSCSI, você precisa concluir os itens a seguir.

- Crie um FSx para o sistema de arquivos ONTAP. Para obter mais informações, consulte Criar sistemas de arquivos.
- Crie uma LUN de iSCSI no sistema de arquivos. Para obter mais informações, consulte Como criar um LUN de iSCSI.
- Crie uma EC2 instância executando a Amazon Machine Image (AMI) do Amazon Linux 2 na mesma VPC do sistema de arquivos. Esse é o host Linux no qual você configurará o iSCSI e acessará os dados do arquivo.

  Além do escopo desses procedimentos, se o host estiver localizado em outra VPC, você poderá usar o emparelhamento de VPC ou conceder outro VPCs acesso AWS Transit Gateway aos endpoints iSCSI do volume. Para obter mais informações, consulte Acesso a dados de fora da VPC de implantação.
- Configure os grupos de segurança de VPC do host do Linux para permitir tráfego de entrada e saída, conforme descrito em Controle de acesso ao sistema de arquivos com a Amazon VPC.

- Obtenha as credenciais para o ONTAP usuário com `fsxadmin` privilégios que você usará para acessar o ONTAP CLI. Para obter mais informações, consulte Usuários e perfis do ONTAP.
- O host Linux que você configurará para iSCSI e usará para acessar o sistema de arquivos FSx for ONTAP está localizado na mesma VPC e. Conta da AWS
- Recomendamos que a EC2 instância esteja na mesma zona de disponibilidade da sub-rede preferencial do seu sistema de arquivos, conforme mostrado no gráfico a seguir.



Se sua EC2 instância executa uma AMI Linux diferente da Amazon Linux 2, alguns dos utilitários usados nesses procedimentos e exemplos podem já estar instalados, e você pode usar comandos diferentes para instalar os pacotes necessários. Além de instalar pacotes, os comandos usados nesta seção são válidos para outros EC2 Linux AMIs.

Tópicos

- Instalar e configurar iSCSI no host Linux
- Configurar iSCSI no sistema de arquivos FSx for ONTAP
- Montar um LUN de iSCSI no cliente Linux

Instalar e configurar iSCSI no host Linux

Instalar o cliente iSCSI

1. Confirme se `iscsi-initiator-utils` e `device-mapper-multipath` estão instalados no seu dispositivo Linux. Conecte-se à instância do Linux usando um cliente SSH. Para obter mais informações, consulte Connect to your Linux instance using SSH.
2. Instale `multipath` e o cliente iSCSI usando o comando a seguir. A instalação de `multipath` é necessária se quiser fazer o failover automático entre os servidores de arquivos.

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. Para facilitar uma resposta mais rápida ao fazer o failover automático entre servidores de arquivos ao usar `multipath`, defina o valor do tempo limite de substituição no arquivo `/etc/iscsi/iscsid.conf` como um valor de `5` em vez de usar o valor padrão de `120`.

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/
node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/
iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. Inicie o serviço iSCSI.

```
~$ sudo service iscsid start
```

   Observe que, dependendo da sua versão do Linux, talvez precise usar este comando:

```
~$ sudo systemctl start iscsid
```

5. Confirme se o serviço está em execução usando o comando a seguir.

```
~$ sudo systemctl status iscsid.service
```

   O sistema responde com a seguinte saída:

```
iscsid.service - Open-iSCSI
    Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor
 preset: disabled)
    Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
    Docs: man:iscsid(8)
```

```
    man:iscsiadm(8)
    Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
    CGroup: /system.slice/iscsid.service
    ##14659 /usr/sbin/iscsid
    ##14660 /usr/sbin/iscsid
```

Configurar o iSCSI no seu cliente Linux

1. Para permitir que seus clientes façam o failover automático entre os servidores de arquivos, é necessário configurar múltiplos caminhos. Use o seguinte comando:

   ```
   ~$ sudo mpathconf --enable --with_multipathd y
   ```

2. Determine o nome do iniciador do host do Linux usando o comando a seguir. A localização do nome do iniciador depende do utilitário do iSCSI. Se estiver usando `iscsi-initiator-utils`, o nome do iniciador está localizado no arquivo `/etc/iscsi/initiatorname.iscsi`.

   ```
   ~$ sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   O sistema responde com o nome do iniciador.

   ```
   InitiatorName=iqn.1994-05.com.redhat:abcdef12345
   ```

Configurar iSCSI no sistema de arquivos FSx for ONTAP

1. Conecte-se à CLI do NetApp ONTAP no FSx sistema de arquivos for ONTAP no qual você criou o LUN iSCSI usando o comando a seguir. Para obter mais informações, consulte Usar o NetApp ONTAP CLI.

   ```
   ~$ ssh fsxadmin@your_management_endpoint_ip
   ```

2. Crie o grupo iniciador (`igroup`) usando o comando NetApp ONTAP CLI. lun igroup create
   Um grupo de iniciadores mapeia para LUNs iSCSI e controla a quais iniciadores (clientes) têm acesso. LUNs Substitua `host_initiator_name` pelo nome do iniciador do host do Linux que você recuperou no procedimento anterior.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype linux
```

Se você quiser disponibilizar o LUNs mapeado para esse igroup para vários hosts, você pode especificar vários nomes de iniciadores separados por uma vírgula. Para obter mais informações, consulte lun igroup create no Centro de Documentação do NetApp ONTAP.

3. Confirme se o `igroup` existe usando o comando lun igroup show:

```
::> lun igroup show
```

O sistema responde com a seguinte saída:

```
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
svm_name  igroup_name  iscsi    linux    iqn.1994-05.com.redhat:abcdef12345
```

4. Esta etapa pressupõe que você já tenha criado um LUN de iSCSI. Se você não tiver, consulte step-by-step as instruções Como criar um LUN de iSCSI para fazer isso.

   Crie um mapeamento do LUN criado para o igroup que você criou, usando o lun mapping create, especificando os atributos a seguir.

   - *svm_name*: o nome da máquina virtual de armazenamento que fornece o destino iSCSI. O host usa esse valor para acessar o LUN.
   - *vol_name*: o nome do volume que hospeda o LUN.
   - *lun_name*: o nome que você atribuiu ao LUN.
   - *igroup_name*: o nome do grupo de iniciadores.
   - *lun_id*: o número inteiro do ID do LUN é específico do mapeamento e não do LUN em si. Isso é usado pelos iniciadores no igroup, pois o número da unidade lógica usa esse valor para o iniciador ao acessar o armazenamento.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Use o comando `lun show -path` para confirmar se o LUN foi criado, on-line e mapeado.

```
::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
```

O sistema responde com a seguinte saída:

```
 Vserver    Path                            serial-hex               state    mapped
 --------- ------------------------------- ------------------------ --------
 --------
 svm_name  /vol/vol_name/lun_name          6c5742314e5d52766e796150 online   mapped
```

Salve o valor `serial_hex` (neste exemplo, é `6c5742314e5d52766e796150`). Você o usará em uma etapa posterior para criar um nome fácil para o dispositivo de blocos.

6. Use o comando `network interface show -vserver` para recuperar os endereços das interfaces `iscsi_1` e `iscsi_2` e da SVM na qual você criou o LUN do iSCSI.

```
::> network interface show -vserver svm_name
```

O sistema responde com a seguinte saída:

```
            Logical               Status     Network            Current
        Current Is
Vserver     Interface             Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------            ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.0.143/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.21.81/20
 FSxId0123456789abcdef8-02  e0e     true
            nfs_smb_management_1
                                  up/up      198.19.250.177/20
 FSxId0123456789abcdef8-01  e0e     true
3 entries were displayed.
```

Neste exemplo, o endereço IP de `iscsi_1` é `172.31.0.143` e `iscsi_2` é `172.31.21.81`.

Montar um LUN de iSCSI no cliente Linux

O processo de montagem da LUN iSCSI no cliente Linux envolve três etapas:

1. Descobrir os nós iSCSI de destino
2. Particionar a LUN iSCSI
3. Montar a LUN iSCSI no cliente

Isso é abordado nos procedimentos a seguir.

Para descobrir os nós iSCSI de destino

1. Em seu cliente Linux, use o comando a seguir para descobrir os nós iSCSI de destino usando o `iscsi_1` endereço IP. *`iscsi_1_IP`*

   ```
   ~$ sudo iscsiadm --mode discovery --op update --type sendtargets --
   portal iscsi_1_IP
   ```

   ```
   172.31.0.143:3260,1029
    iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
   172.31.21.81:3260,1028
    iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
   ```

   Neste exemplo, `iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3` corresponde ao `target_initiator` para o LUN do iSCSI na zona de disponibilidade preferencial.

2. (Opcional) Para gerar uma taxa de transferência maior do que o máximo de 5 Gbps (~ 625) do cliente EC2 único da Amazon MBps para seu LUN iSCSI, siga os procedimentos descritos em Largura de banda de EC2 rede de instâncias da Amazon no Guia do usuário do Amazon Elastic Compute Cloud para instâncias Linux para estabelecer sessões adicionais para maior taxa de transferência.

   O comando a seguir estabelece 8 sessões por iniciador por nó ONTAP em cada zona de disponibilidade, permitindo que o cliente direcione até 40 Gbps (5.000 MBps) de taxa de transferência agregada para o LUN iSCSI.

```
~$ sudo iscsiadm --mode node -T target_initiator --op update -n
 node.session.nr_sessions -v 8
```

3. Faça login nos iniciadores de destino. Seus iSCSI LUNs são apresentados como discos disponíveis.

```
~$ sudo iscsiadm --mode node -T target_initiator --login
```

```
Logging in to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] (multiple)
Login to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] successful.
```

A saída acima está truncada; você deve ver uma resposta `Logging in` e uma resposta `Login successful` para cada sessão em cada servidor de arquivos. No caso de quatro sessões por nó, haverá 8 respostas `Logging in` e 8 respostas `Login successful`.

4. Use o comando a seguir para verificar se `dm-multipath` identificou e mesclou as sessões de iSCSI mostrando um único LUN com várias políticas. Deve haver um número igual de dispositivos listados como `active` e aqueles listados como `enabled`.

```
~$ sudo multipath -ll
```

Na saída, o nome do disco é formatado como `dm-xyz`, onde `xyz` é um número inteiro. Se não houver outros discos de múltiplos caminhos, o valor será `dm-0`.

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
 hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda     8:0   active ready running
| |- 1:0:0:1 sdc     8:32  active ready running
| |- 3:0:0:1 sdg     8:96  active ready running
| `- 4:0:0:1 sdh     8:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb     8:16  active ready running
  |- 7:0:0:1 sdf     8:80  active ready running
```

```
  |- 6:0:0:1 sde     8:64  active ready running
  `- 5:0:0:1 sdd     8:48  active ready running
```

Seu dispositivo de blocos agora está conectado ao cliente Linux. Ele está localizado sob o caminho `/dev/`*`dm-xyz`*. Você não deve usar esse caminho para fins administrativos; em vez disso, use o link simbólico que está sob o caminho `/dev/mapper/`*`wwid`*, onde *`wwid`* é um identificador exclusivo do seu LUN que é consistente em todos os dispositivos. Na próxima etapa, você fornecerá um nome fácil para *`wwid`*, de modo que possa diferenciá-lo de outros discos com múltiplos caminhos.

Para dar um nome amigável ao dispositivo de blocos

1. Para fornecer um nome fácil ao dispositivo, crie um alias no arquivo `/etc/multipath.conf`. Para isso, adicione a seguinte entrada ao arquivo usando seu editor de texto preferencial, substituindo os seguintes espaços reservados:

   - Substitua `serial_hex` pelo valor salvo no procedimento Configurar iSCSI no sistema de arquivos FSx for ONTAP.
   - Adicione o prefixo `3600a0980` ao valor `serial_hex` conforme mostrado no exemplo. Este é um preâmbulo exclusivo para a distribuição NetApp ONTAP que o Amazon FSx for NetApp ONTAP usa.
   - Substitua `device_name` pelo nome fácil que deseja usar no seu dispositivo.

   ```
   multipaths {
       multipath {
           wwid 3600a0980serial_hex
           alias device_name
       }
   }
   ```

   Como alternativa, você pode copiar e salvar o script a seguir como um arquivo bash, como `multipath_alias.sh`. Você pode executar o script com privilégios sudo, substituindo *`serial_hex`* (sem o prefixo 3600a0980) e *`device_name`* pelo seu respectivo número de série e pelo nome desejado. Esse script busca uma seção `multipaths` não comentada no arquivo `/etc/multipath.conf`. Se a seção existir, ele anexa uma entrada `multipath` a essa seção; caso contrário, ele criará uma seção `multipaths` com uma entrada `multipath` para o seu dispositivo de blocos.

```
#!/bin/bash
SN=serial_hex
ALIAS=device_name
CONF=/etc/multipath.conf
grep -q '^multipaths {' $CONF
UNCOMMENTED=$?
if [ $UNCOMMENTED -eq 0 ]
then
        sed -i '/^multipaths {/a\\tmultipath {\n\t\twwid 3600a0980'"${SN}"'\n\t
\talias '"${ALIAS}"'\n\t}\n' $CONF
else
        printf "multipaths {\n\tmultipath {\n\t\twwid 3600a0980$SN\n\t\talias
 $ALIAS\n\t}\n}" >> $CONF
fi
```

2. Reinicie o serviço `multipathd` para que as alterações em `/etc/multipathd.conf` entrem em vigor.

```
~$ systemctl restart multipathd.service
```

Particionar o LUN

A próxima etapa é formatar e particionar o LUN usando `fdisk`.

1. Use o comando a seguir para verificar se o caminho para `device_name` está presente.

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. Particione o disco usando `fdisk`. Você inserirá um prompt interativo. Insira as opções na ordem mostrada. Você pode criar várias partições usando um valor menor que o último setor (`20971519`, neste exemplo).

> **Note**
>
> O valor de `Last sector` terá variações, dependendo do tamanho do LUN de iSCSI (10 GB, neste exemplo).

```
~$ sudo fdisk /dev/mapper/device_name
```

O prompt interativo `fsdisk` é iniciado.

```
Welcome to fdisk (util-linux 2.30.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
 20971519): 20971519

Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

Após inserir `w`, sua nova partição `/dev/mapper/partition_name` fica disponível. O *partition_name* tem o formato *<device_name><partition_number>*. 1foi usado como o número da partição usado no `fdisk` comando na etapa anterior.

3. Crie seu sistema de arquivos usando `/dev/mapper/partition_name` como caminho.

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

O sistema responde com a seguinte saída:

```
mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
```

```
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Montar o LUN no cliente Linux

1. Crie um diretório *directory_path* como ponto de montagem para seu sistema de arquivos.

```
~$ sudo mkdir /directory_path/mount_point
```

2. Monte o sistema de arquivos usando o comando a seguir.

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. (Opcional) Se você quiser dar a um usuário específico a propriedade do diretório de montagem, substitua *username* pelo nome de usuário do proprietário.

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (Opcional) Verifique se pode ler e gravar dados no sistema de arquivos.

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

Você criou e montou com êxito um LUN de iSCSI no cliente Linux.

Provisionamento de iSCSI para Windows

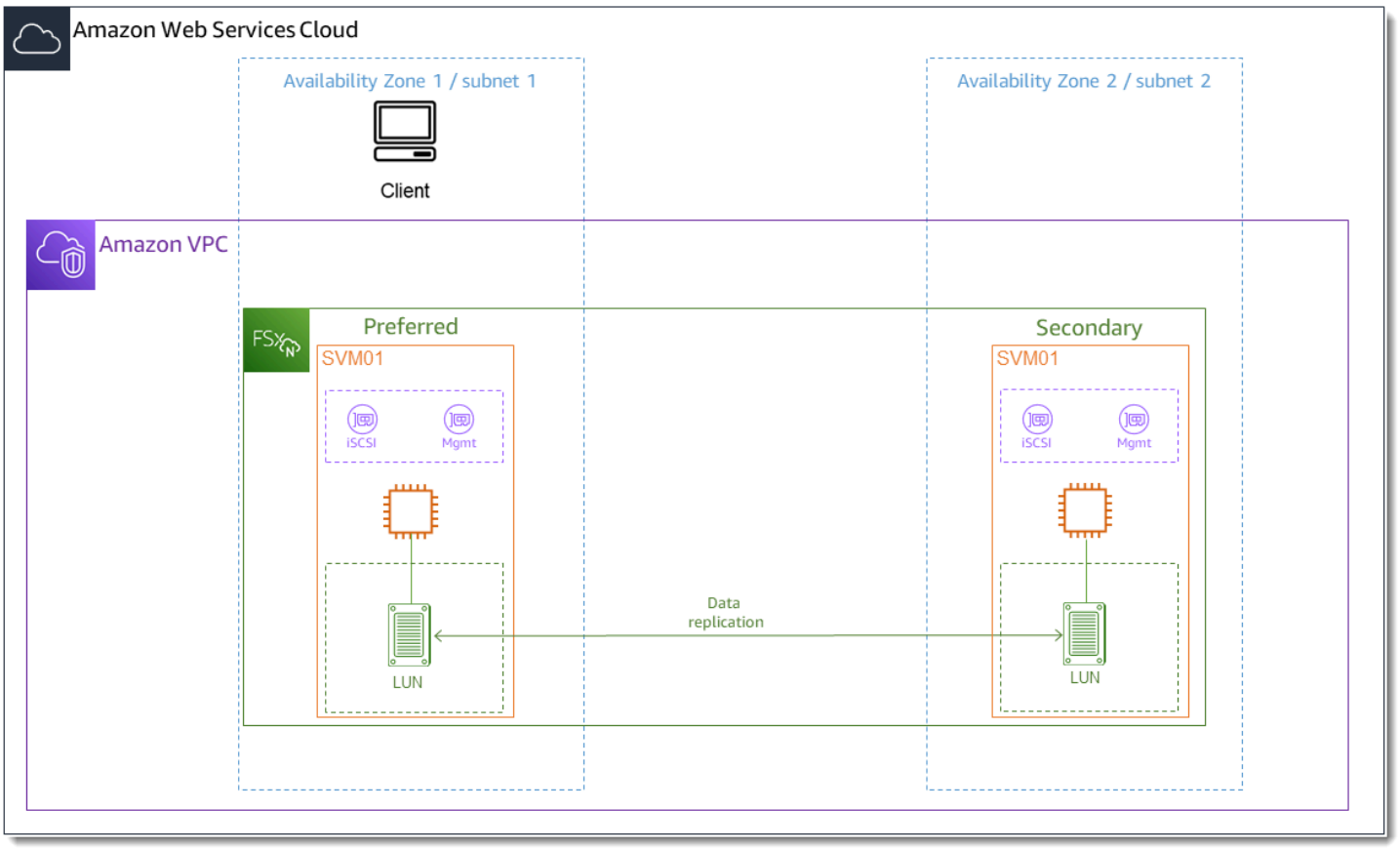
FSx for ONTAP suporta o protocolo iSCSI. Você precisa provisionar iSCSI no cliente Windows e na SVM e no volume para usar o protocolo iSCSI para transportar dados entre clientes e seu sistema de arquivos. O protocolo iSCSI está disponível em todos os sistemas de arquivos com até 6 pares de alta disponibilidade (HA).

Os exemplos apresentados nesses procedimentos mostram como provisionar o protocolo iSCSI no cliente e no sistema FSx de arquivos ONTAP e usar a seguinte configuração:

- O LUN do iSCSI que está sendo montado em um host do Windows já foi criado. Para obter mais informações, consulte Como criar um LUN de iSCSI.
- O host Microsoft Windows que está montando o LUN iSCSI é uma EC2 instância da Amazon executando uma Amazon Machine Image (AMI) do Microsoft Windows Server 2019. Ele tem grupos de segurança de VPC configurados para permitir tráfego de entrada e saída, conforme descrito em Controle de acesso ao sistema de arquivos com a Amazon VPC.

  Você pode estar usando uma AMI diferente do Microsoft Windows na configuração.
- O cliente e o sistema de arquivos estão localizados na mesma VPC e Conta da AWS. Se o cliente estiver localizado em outra VPC, você poderá usar o emparelhamento de VPC ou AWS Transit Gateway conceder outro acesso VPCs aos endpoints iSCSI. Para obter mais informações, consulte Acesso a dados de fora da VPC de implantação.

  Recomendamos que a EC2 instância esteja na mesma zona de disponibilidade da sub-rede preferencial do seu sistema de arquivos, conforme mostrado no gráfico a seguir.



Tópicos

- Configurar o iSCSI no cliente Windows
- Configurar iSCSI no sistema de arquivos FSx for ONTAP
- Monte um LUN de iSCSI no cliente Windows
- Validar sua configuração do iSCSI

Configurar o iSCSI no cliente Windows

1. Use a Área de Trabalho Remota do Windows para se conectar ao cliente Windows no qual você deseja montar o LUN de iSCSI. Para obter mais informações, consulte Conectar-se à sua instância baseada no Windows usando RDP no Guia do usuário do Amazon Elastic Compute Cloud.
2. Abra um Windows PowerShell como administrador. Use os comandos a seguir para habilitar o iSCSI na sua instância do Windows e configurar o serviço de iSCSI para iniciar automaticamente.

```
PS C:\> Start-Service MSiSCSI
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. Recupere o nome do iniciador da instância do Windows. Você usará esse valor na configuração do iSCSI em FSx seu sistema de arquivos for ONTAP usando a NetApp CLI ONTAP.

   ```
   PS C:\> (Get-InitiatorPort).NodeAddress
   ```

   O sistema responde com a porta do iniciador:

   ```
   iqn.1991-05.com.microsoft:ec2amaz-abc123d
   ```

4. Para permitir que seus clientes façam o failover automático entre os servidores de arquivos, é necessário instalar `Multipath-IO` (MPIO) na instância do Windows. Use o seguinte comando:

   ```
   PS C:\> Install-WindowsFeature Multipath-IO
   ```

5. Reinicie a instância do Windows após concluir a instalação de `Multipath-IO`. Mantenha a instância do Windows aberta para executar as etapas de montagem do LUN de iSCSI na seção a seguir.

Configurar iSCSI no sistema de arquivos FSx for ONTAP

1. Para acessar o ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Usar o ONTAP CLI lun igroup create, crie o grupo iniciador ou. `igroup` Um grupo de iniciadores mapeia para LUNs iSCSI e controla a quais iniciadores (clientes) têm acesso. LUNs Substitua `host_initiator_name` pelo nome do iniciador do host do Windows recuperado no procedimento anterior.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype windows
```

Para `igroup` disponibilizar o LUNs mapeado para isso para vários hosts, você pode especificar vários nomes de iniciadores separados por vírgula usando `lun igroup create` ONTAP Comando CLI.

3. Confirme se o `igroup` foi criado com sucesso usando o lun igroup show ONTAP Comando da CLI:

```
::> lun igroup show
```

O sistema responde com a seguinte saída:

```
Vserver    Igroup        Protocol OS Type  Initiators
---------  ------------  -------- -------- ------------------------------------
svm_name   igroup_name   iscsi    windows  iqn.1994-05.com.windows:abcdef12345
```

Com o `igroup` criado, você está pronto para criá-los LUNs e mapeá-los para `igroup` o.

4. Esta etapa pressupõe que você já tenha criado um LUN de iSCSI. Caso contrário, consulte step-by-step as instruções Como criar um LUN de iSCSI para fazer isso.

Crie um mapeamento de LUN do LUN para o seu novo `igroup`.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Confirme se o LUN foi criado on-line e mapeado com o seguinte comando:

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

Agora, você já pode adicionar o destino iSCSI na sua instância do Windows.

6. Recupere os endereços IP das interfaces `iscsi_1` e `iscsi_2` da SVM usando o seguinte comando:

```
::> network interface show -vserver svm_name
```

```
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
svm_name
            iscsi_1    up/up      172.31.0.143/20    FSxId0123456789abcdef8-01
                                                                   e0e     true
            iscsi_2    up/up      172.31.21.81/20    FSxId0123456789abcdef8-02
                                                                   e0e     true
            nfs_smb_management_1
                       up/up      198.19.250.177/20  FSxId0123456789abcdef8-01
                                                                   e0e     true
3 entries were displayed.
```

Neste exemplo, o endereço IP de `iscsi_1` é `172.31.0.143` e `iscsi_2` é `172.31.21.81`.

Monte um LUN de iSCSI no cliente Windows

1. Na sua instância do Windows, abra um PowerShell terminal como administrador.
2. Você criará um script `.ps1` que faça o seguinte:

   - Conecta-se a cada uma das interfaces de iSCSI do seu sistema de arquivos.
   - Adiciona e configura o MPIO para o iSCSI.
   - Estabelece 8 sessões para cada conexão iSCSI, o que permite ao cliente direcionar até 40 Gbps (MBps5.000) de taxa de transferência agregada para o LUN iSCSI. Ter 8 sessões garante que um único cliente possa impulsionar a capacidade total de 4.000 MBps taxas de transferência para o nível mais alto FSx de capacidade de transferência do ONTAP. Opcionalmente, você pode alterar o número de sessões para um número maior ou menor de sessões (cada sessão fornece até 625 MBps de taxa de transferência) modificando a variável. `RecommendedConnectionCount` Para obter mais informações, consulte a largura de banda da rede de EC2 instâncias da Amazon no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Windows.

   Copie o conjunto de comandos a seguir em um arquivo para criar o script `.psl`.

- Substitua `iscsi_1` e `iscsi_2` pelos endereços IP recuperados na etapa anterior.
- Substitua `ec2_ip` pelo endereço IP da instância do Windows.

```
Write-Host "Starting iSCSI connection setup..."
     $TargetPortalAddresses = @("iscsi_1","iscsi_2"); $LocaliSCSIAddress = "ec2_ip"
     $RecommendedConnectionCount = 8

     Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
         New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
     }

     New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

     $currentMPIOSettings = Get-MPIOSetting
     if ($currentMPIOSettings.PathVerificationState -ne 'Enabled') {
         Write-Host "Setting MPIO path verification state to Enabled"; Set-
MPIOSetting -NewPathVerificationState Enabled
     } else { Write-Host "MPIO path verification state already Enabled" }

     $portalConnectionCounts = @{}
     foreach ($TargetPortalAddress in $TargetPortalAddresses)
 { $portalConnectionCounts[$TargetPortalAddress] = 0 }

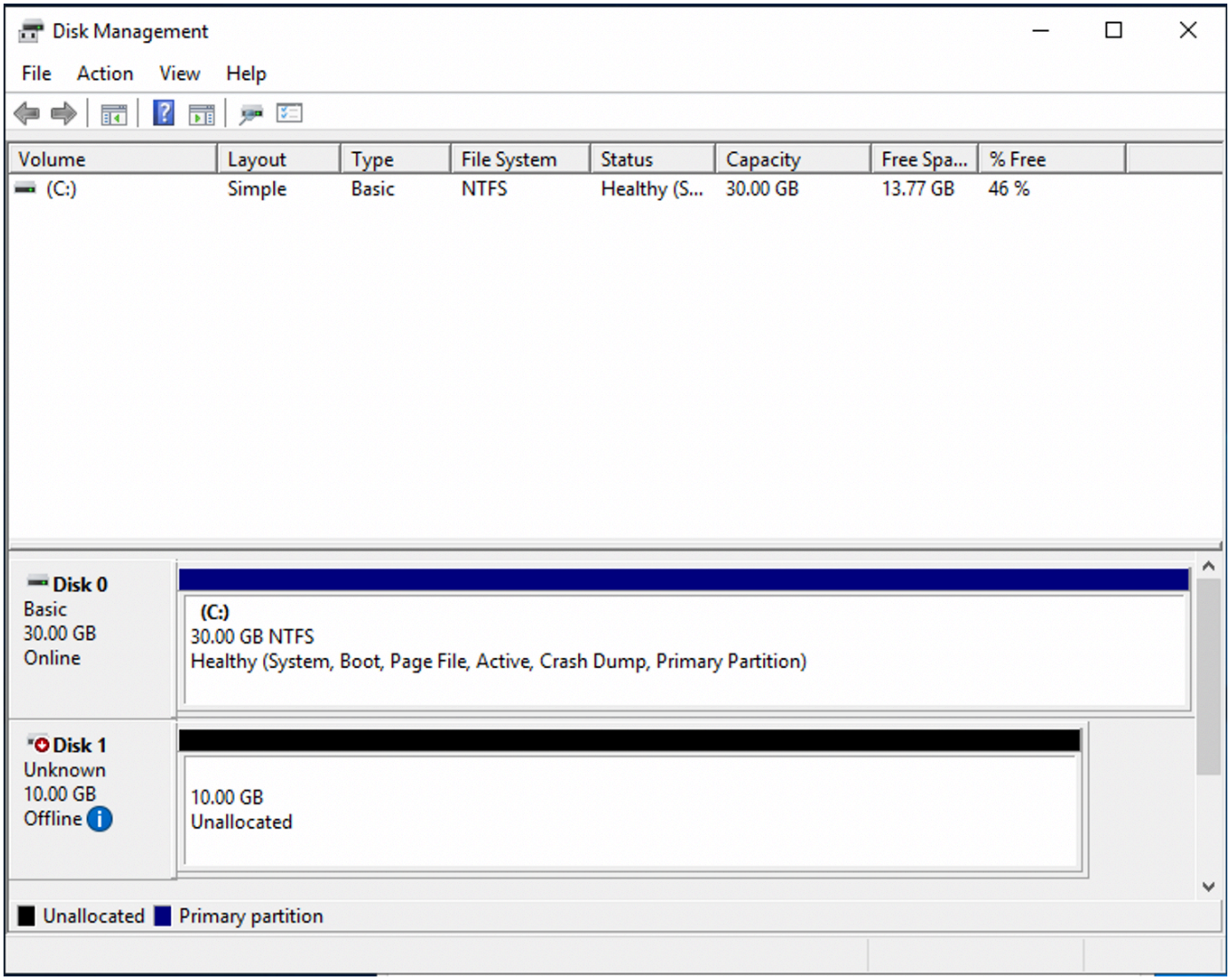
     $sessions = Get-IscsiSession
     if ($sessions) {
         foreach ($session in $sessions) {
             if ($session.IsConnected) {
                 $targetPortal = (Get-IscsiTargetPortal -iSCSISession
 $session).TargetPortalAddress
                 if ($portalConnectionCounts.ContainsKey($targetPortal))
 { $portalConnectionCounts[$targetPortal]++ }
             }
         }
     }

     foreach ($TargetPortalAddress in $TargetPortalAddresses) {
         $existingCount = $portalConnectionCounts[$TargetPortalAddress];
 $remainingConnections = $RecommendedConnectionCount - $existingCount
```

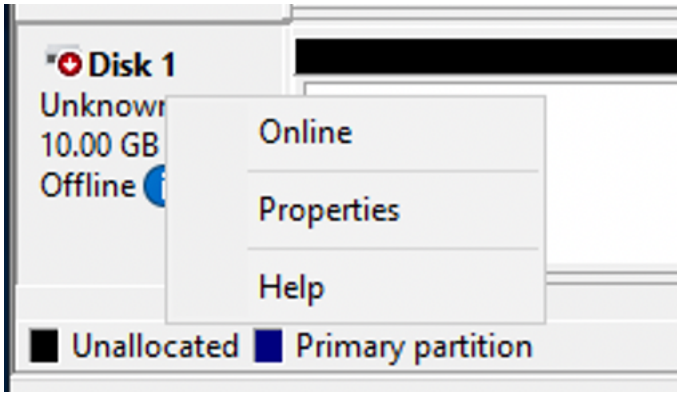
```
        Write-Host "Portal $TargetPortalAddress has $existingCount
 existing connections, $remainingConnections remaining (max recommended:
 $RecommendedConnectionCount)"
        if ($remainingConnections -gt 0) {
            Write-Host "Creating $remainingConnections connections for portal
 $TargetPortalAddress"
            1..$remainingConnections | ForEach-Object {
                Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true
            }
        } else { Write-Host "Maximum connections (8) reached for portal
 $TargetPortalAddress" }
    }

    Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

3. Inicie a aplicação Gerenciamento de Disco do Windows. Abra a caixa de diálogo Run do Windows, insira `diskmgmt.msc` e pressione Enter. A aplicação Gerenciamento de Disco se abre.



4. Localize o disco não alocado. Esse é o LUN de iSCSI. No exemplo, Disk 1 é o disco iSCSI. Está off-line.



Coloque o volume on-line posicionando o cursor sobre Disk 1, clique com o botão direito do mouse e escolha On-line.

> **Note**
>
> Você pode modificar a política da rede de área do armazenamento (SAN) para que novos volumes sejam automaticamente colocados on-line. Para obter mais informações, consulte as políticas da SAN na Microsoft Windows Server Command Reference.

5. Para inicializar o disco, coloque o cursor sobre Disk 1, clique com o botão direito do mouse e escolha Inicializar. A caixa de diálogo Inicializar é exibida. Escolha OK para inicializar o disco.
6. Formate o disco como você faria normalmente. Depois que a formatação estiver concluída, o drive do iSCSI aparecerá como um drive utilizável no cliente Windows.

Validar sua configuração do iSCSI

Disponibilizamos um script para verificar se a configuração do iSCSI está correta. O script examina parâmetros como contagem de sessões, distribuição de nós e status de E/S do Multipath (MPIO). A tarefa a seguir explica como instalar e usar o script.

Para validar sua configuração do iSCSI

1. Abra uma PowerShell janela do Windows.
2. Faça download do script usando o comando a seguir.

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/
samples/CheckiSCSI.zip" -OutFile "CheckiSCSI.zip"
```

3. Faça download do arquivo zip usando o comando a seguir.

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

4. Execute o script usando o comando a seguir.

```
PS C:\> ./CheckiSCSI.ps1
```

5. Revise a saída para entender o estado atual da sua configuração. O exemplo a seguir demonstra uma configuração bem-sucedida do iSCSI.

```
PS C:\> ./CheckiSCSI.ps1
```

```
This script checks the iSCSI configuration on the local instance.
It will provide information about the number of connected sessions, connected file
 servers, and MPIO status.

MPIO is installed on this server.

MPIO Load Balance Policy is set to Round Robin (RR).
Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'
has 16 total sessions (16 active, 0 non-active)
spread across 2 node(s).
MPIO: Yes
```

Provisionamento NVMe /TCP para Linux

FSx para ONTAP suporta o Non-Volatile Memory Express sobre TCP (NVMe/TCP) block storage protocol. With NVMe/TCP, você usa o ONTAP CLI para provisionar namespaces e subsistemas e, em seguida, mapear os namespaces para subsistemas, da mesma forma como LUNs são provisionados e mapeados para grupos de iniciadores (igroups) para iSCSI. O protocolo NVMe /TCP está disponível em sistemas de arquivos de segunda geração que têm 6 ou menos pares de alta disponibilidade (HA).

> **Note**
>
> FSx para sistemas de arquivos ONTAP, use os endpoints iSCSI de um SVM para os protocolos de armazenamento em blocos NVMe iSCSI e /TCP.

Há três etapas principais para processar a configuração de NVMe /TCP em seu Amazon FSx para NetApp ONTAP, que são abordadas nos seguintes procedimentos:

1. Instale e configure o NVMe cliente no host Linux.
2. Configure NVMe no SVM do sistema de arquivos.
   - Crie um NVMe namespace.
   - Crie um NVMe subsistema.

- Mapeie o namespace para o subsistema.
- Adicione o NQN do cliente ao subsistema.

3. Monte um NVMe dispositivo no cliente Linux.

Antes de começar

Antes de iniciar o processo de configuração do sistema de arquivos para NVMe /TCP, você precisa ter os seguintes itens concluídos.

- Crie um FSx para o sistema de arquivos ONTAP. Para obter mais informações, consulte Criar sistemas de arquivos.
- Crie uma EC2 instância executando o Red Hat Enterprise Linux (RHEL) 9.3 na mesma VPC do sistema de arquivos. Esse é o host Linux no qual você configurará NVMe e acessará seus dados de arquivo usando NVMe /TCP para Linux.

  Além do escopo desses procedimentos, se o host estiver localizado em outra VPC, você poderá usar o emparelhamento de VPC ou conceder outro VPCs acesso AWS Transit Gateway aos endpoints iSCSI do volume. Para obter mais informações, consulte Acesso a dados de fora da VPC de implantação.
- Configure os grupos de segurança de VPC do host do Linux para permitir tráfego de entrada e saída, conforme descrito em Controle de acesso ao sistema de arquivos com a Amazon VPC.
- Obtenha as credenciais para o ONTAP usuário com `fsxadmin` privilégios que você usará para acessar o ONTAP CLI. Para obter mais informações, consulte Usuários e perfis do ONTAP.
- O host Linux que você configurará NVMe e usará para acessar o sistema de arquivos FSx for ONTAP está localizado na mesma VPC e. Conta da AWS
- Recomendamos que a EC2 instância esteja na mesma zona de disponibilidade da sub-rede preferencial do seu sistema de arquivos.

Se sua EC2 instância executa uma AMI Linux diferente da RHEL 9.3, alguns dos utilitários usados nesses procedimentos e exemplos podem já estar instalados, e você pode usar comandos diferentes para instalar os pacotes necessários. Além de instalar pacotes, os comandos usados nesta seção são válidos para outros EC2 Linux AMIs.

Tópicos

- Instale e configure NVMe no host Linux

- Configurar NVMe no sistema de arquivos FSx for ONTAP
- Monte um NVMe dispositivo em seu cliente Linux

Instale e configure NVMe no host Linux

Para instalar o NVMe cliente

1. Conecte-se à instância do Linux usando um cliente SSH. Para obter mais informações, consulte Conectar-se à instância do Linux usando um cliente SSH.
2. Instale o `nvme-cli` usando o comando a seguir:

```
~$ sudo yum install -y nvme-cli
```

3. Carregue o módulo `nvme-tcp` no host:

```
$ sudo modprobe nvme-tcp
```

4. Obtenha o Nome NVMe Qualificado (NQN) do host Linux usando o seguinte comando:

```
$ cat /etc/nvme/hostnqn
nqn.2014-08.org.nvmexpress:uuid:9ed5b327-b9fc-4cf5-97b3-1b5d986345d1
```

   Registre a resposta para uso em uma etapa posterior.

Configurar NVMe no sistema de arquivos FSx for ONTAP

Para configurar NVMe no sistema de arquivos

Conecte-se à CLI do NetApp ONTAP no sistema de arquivos FSx do ONTAP no qual você planeja criar NVMe o (s) dispositivo (s).

1. Para acessar o ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Crie um novo volume no SVM que você está usando para acessar a NVMe interface.

```
::> vol create -vserver fsx -volume nvme_vol1 -aggregate aggr1 -size 1t
     [Job 597] Job succeeded: Successful
```

3. Crie o NVMe namespace ns_1 usando o comando vserver nvme namespace create NetApp ONTAP CLI. Um namespace mapeia para iniciadores (clientes) e controla quais iniciadores (clientes) têm acesso aos dispositivos. NVMe

```
::> vserver nvme namespace create -vserver fsx -path /vol/nvme_vol1/ns_1 -size 100g
 -ostype linux
Created a namespace of size 100GB (107374182400).
```

4. Crie o NVMe subsistema usando o comando vserver nvme subsystem create NetApp ONTAP CLI.

```
~$ vserver nvme subsystem create -vserver fsx -subsystem sub_1 -ostype linux
```

5. Mapeie o namespace para o subsistema que acaba de criar.

```
::> vserver nvme subsystem map add -vserver fsx -subsystem sub_1 -path /vol/
nvme_vol1/ns_1
```

6. Adicione o cliente ao subsistema usando o NQN que você recuperou anteriormente.

```
::> vserver nvme subsystem host add -subsystem sub_1 -host-nqn
 nqn.2014-08.org.nvmexpress:uuid:ec21b083-1860-d690-1f29-44528e4f4e0e -vserver fsx
```

Se quiser disponibilizar os dispositivos mapeados para esse subsistema a vários hosts, você pode especificar vários nomes de iniciadores em uma lista separada por vírgula. Para obter mais informações, consulte vserver nvme subsystem host add na documentação do ONTAP. NetApp

7. Confirme a existência do namespace usando o comando vserver nvme namespace show:

```
::> vserver nvme namespace show -vserver fsx -instance
Vserver Name: fsx
            Namespace Path: /vol/nvme_vol1/ns_1
                      Size: 100GB
                 Size Used: 90.59GB
```

```
                    OS Type: linux
                    Comment:
                 Block Size: 4KB
                      State: online
          Space Reservation: false
Space Reservations Honored: false
               Is Read Only: false
             Creation Time: 5/20/2024 17:03:08
            Namespace UUID: c51793c0-8840-4a77-903a-c869186e74e3
                 Vdisk ID: 80d42c6f00000000187cca9
      Restore Inaccessible: false
   Inconsistent Filesystem: false
       Inconsistent Blocks: false
                   NVFail: false
Node Hosting the Namespace: FsxId062e9bb6e05143fcb-01
               Volume Name: nvme_vol1
                Qtree Name:
          Mapped Subsystem: sub_1
            Subsystem UUID: db526ec7-16ca-11ef-a612-d320bd5b74a9
              Namespace ID: 00000001h
              ANA Group ID: 00000001h
              Vserver UUID: 656d410a-1460-11ef-a612-d320bd5b74a9
                Vserver ID: 3
               Volume MSID: 2161388655
               Volume DSID: 1029
                 Aggregate: aggr1
            Aggregate UUID: cfa8e6ee-145f-11ef-a612-d320bd5b74a9
 Namespace Container State: online
        Autodelete Enabled: false
          Application UUID: -
               Application: -
  Has Metadata Provisioned: true

1 entries were displayed.
```

8. Use o network interface show -vservercomando para recuperar os endereços das interfaces de armazenamento em bloco da SVM na qual você criou seus NVMe dispositivos.

```
::> network interface show -vserver svm_name -data-protocol nvme-tcp
            Logical              Status     Network            Current
        Current Is
Vserver     Interface            Admin/Oper Address/Mask       Node
        Port    Home
```

```
----------- ----------           ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.16.19/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.26.134/20
 FSxId0123456789abcdef8-02  e0e     true
2 entries were displayed.
```

> **Note**
>
> O `iscsi_1` LIF é usado tanto para NVMe iSCSI quanto para /TCP.

Neste exemplo, o endereço IP de iscsi_1 é 172.31.16.19 e de iscsi_2 é 172.31.26.134.

Monte um NVMe dispositivo em seu cliente Linux

O processo de montagem do NVMe dispositivo em seu cliente Linux envolve três etapas:

1. Descobrindo os nós NVMe
2. Particionando o dispositivo NVMe
3. Montando o NVMe dispositivo no cliente

Isso é abordado nos procedimentos a seguir.

Para descobrir os NVMe nós de destino

1. Em seu cliente Linux, use o comando a seguir para descobrir os NVMe nós de destino. Substitua *`iscsi_1_IP`* pelo endereço IP de `iscsi_1` e *`client_IP`* pelo endereço IP do cliente.

   > **Note**
   >
   > `iscsi_1`e `iscsi_2` LIFs são usados tanto para iSCSI quanto para armazenamento. NVMe

```
~$ sudo nvme discover -t tcp -w client_IP -a iscsi_1_IP
```

```
Discovery Log Number of Records 4, Generation counter 11
=====Discovery Log Entry 0======
trtype:  tcp
adrfam:  ipv4
subtype: current discovery subsystem
treq:    not specified
portid:  0
trsvcid: 8009
subnqn:  nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr:  172.31.26.134
eflags:  explicit discovery connections, duplicate discovery information
sectype: none
=====Discovery Log Entry 1======
trtype:  tcp
adrfam:  ipv4
subtype: current discovery subsystem
treq:    not specified
portid:  1
trsvcid: 8009
subnqn:  nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr:  172.31.16.19
eflags:  explicit discovery connections, duplicate discovery information
sectype: none
```

2. (Opcional) Para gerar uma taxa de transferência maior do que o máximo de 5 Gbps (~ 625 MBps) do cliente EC2 único da Amazon para seu NVMe dispositivo de arquivo, siga os procedimentos descritos em Largura de banda de rede de EC2 instâncias da Amazon no Guia do usuário do Amazon Elastic Compute Cloud para instâncias Linux para estabelecer sessões adicionais.

3. Faça login nos iniciadores de destino com um tempo limite de perda do controlador de pelo menos 1.800 segundos, mais uma vez usando o endereço IP do `iscsi_1` para *`iscsi_1_IP`*e o endereço IP do cliente para *`client_IP`*. Seus NVMe dispositivos são apresentados como discos disponíveis.

```
~$ sudo nvme connect-all -t tcp -w client_IP -a iscsi_1 -l 1800
```

4. Use o comando a seguir para verificar se a NVMe pilha identificou e mesclou as várias sessões e configurou vários caminhos. Se a configuração tiver sido bem-sucedida, o comando retornará Y.

```
~$ cat /sys/module/nvme_core/parameters/multipath
Y
```

5. Use os comandos a seguir para verificar se a configuração NVMe -oF `model` está definida como `NetApp ONTAP Controller` e o balanceamento de carga `iopolicy` está definido como `round-robin` para o respectivo ONTAP namespaces para distribuir a E/S em todos os caminhos disponíveis

```
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/model
Amazon Elastic Block Store
NetApp ONTAP Controller
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/iopolicy
numa
round-robin
```

6. Use o comando a seguir para verificar se os namespaces foram criados e descobertos corretamente no host:

```
~$ sudo nvme list
Node                  Generic               SN                   Model
                        Namespace  Usage                      Format           FW
 Rev
--------------------- --------------------- --------------------
 ---------------------------------------- ---------- --------------------------
 ---------------- --------
/dev/nvme0n1          /dev/ng0n1            vol05955547c003f0580 Amazon Elastic
 Block Store               0x1         25.77  GB /  25.77  GB    512   B +  0 B
 1.0
/dev/nvme2n1          /dev/ng2n1            lWB12JWY/XLKAAAAAAAC NetApp ONTAP
 Controller                0x1        107.37  GB / 107.37  GB      4 KiB +  0 B
 FFFFFFFF
```

O novo dispositivo na saída é `/dev/nvme2n1`. Esse esquema de nomenclatura pode ser diferente dependendo da instalação do Linux.

7. Verifique se o estado do controlador de cada caminho está ativo e com o status correto de multipathing do Acesso assimétrico a namespace (ANA):

```
~$ nvme list-subsys /dev/nvme2n1
nvme-subsys2 -
 NQN=nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:subsystem.rhel
              hostnqn=nqn.2014-08.org.nvmexpress:uuid:ec2a70bf-3ab2-6cb0-
f997-8730057ceb24
              iopolicy=round-robin
\
 +- nvme2 tcp
 traddr=172.31.26.134,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
 live non-optimized
 +- nvme3 tcp
 traddr=172.31.16.19,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
 live optimized
```

Neste exemplo, a NVMe pilha descobriu automaticamente o LIF alternativo do seu sistema de arquivos`iscsi_2`, 172.31.26.134.

8. Verifique se o NetApp o plug-in exibe os valores corretos para cada ONTAP dispositivo de namespace:

```
~$ sudo nvme netapp ontapdevices -o column
Device           Vserver                   Namespace Path
           NSID UUID                                   Size
---------------- ------------------------
 ------------------------------------------------- ----
 ------------------------------------ ---------
/dev/nvme2n1     fsx                       /vol/nvme_vol1/ns_1
           1    0441c609-3db1-4b0b-aa83-790d0d448ece   107.37GB
```

Para particionar o dispositivo

1. Use o comando a seguir para verificar se o caminho para device_name `nvme2n1` está presente.

```
~$ ls /dev/mapper/nvme2n1
/dev/nvme2n1
```

2. Particione o disco usando `fdisk`. Você inserirá um prompt interativo. Insira as opções na ordem mostrada. Você pode criar várias partições usando um valor menor que o último setor (`20971519`, neste exemplo).

> **Note**
>
> O `Last sector` valor variará dependendo do tamanho do seu NVMe dispositivo (100 GiB neste exemplo).

```
~$ sudo fdisk /dev/mapper/nvme2n1
```

O prompt interativo `fsdisk` é iniciado.

```
Welcome to fdisk (util-linux 2.37.4).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (256-26214399, default 256):
Last sector, +sectors or +size{K,M,G,T,P} (256-26214399, default
 26214399): 20971519

Created a new partition 1 of type 'Linux' and of size 100 GiB.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

Após inserir `w`, sua nova partição `/dev/nvme2n1` fica disponível. O *`partition_name`* tem o formato *`<device_name><partition_number>`*. `1`foi usado como o número da partição no `fdisk` comando na etapa anterior.

3. Crie seu sistema de arquivos usando `/dev/nvme2n1` como caminho.

```
~$ sudo mkfs.ext4 /dev/nvme2n1
```

O sistema responde com a seguinte saída:

```
mke2fs 1.46.5 (30-Dec-2021)
Found a dos partition table in /dev/nvme2n1
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 372fb2fd-ae0e-4e74-ac06-3eb3eabd55fb
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

Para montar o NVMe dispositivo no cliente Linux

1. Crie um diretório *directory_path* como ponto de montagem para seu sistema de arquivos na instância Linux.

   ```
   ~$ sudo mkdir /directory_path/mount_point
   ```

2. Monte o sistema de arquivos usando o comando a seguir.

   ```
   ~$ sudo mount -t ext4 /dev/nvme2n1 /directory_path/mount_point
   ```

3. (Opcional) Se você quiser dar a um usuário específico a propriedade do diretório de montagem, substitua *username* pelo nome de usuário do proprietário.

   ```
   ~$ sudo chown username:username /directory_path/mount_point
   ```

4. (Opcional) Verifique se pode ler e gravar dados no sistema de arquivos.

   ```
   ~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
   ~$ cat directory_path/HelloWorld.txt
   Hello world!
   ```

Você criou e montou com sucesso um NVMe dispositivo no seu cliente Linux.

Provisionamento para Windows NVMe/TCP

FSx para ONTAP suporta o Non-Volatile Memory Express sobre TCP (NVMe/TCP) block storage protocol for Windows. With NVMe/TCP, você usa a ONTAP CLI para provisionar namespaces e subsistemas e, em seguida, mapeia os namespaces para subsistemas, da mesma forma como são LUNs provisionados e mapeados para grupos de iniciadores (igroups) para iSCSI. O NVMe/TCP protocolo está disponível em sistemas de arquivos de segunda geração que têm 6 ou menos pares de alta disponibilidade (HA). .

Para provisionar NVMe/TCP em um host Windows, você precisará baixar um iniciador do fornecedor de sua escolha e seguir as instruções para instalá-lo e provisioná-lo.

Acessar dados com outros serviços da AWS

Além da Amazon EC2, você pode usar outros AWS serviços com seus volumes para acessar seus dados.

Tópicos

- Usando a Amazon WorkSpaces com o FSx ONTAP
- Usando o Amazon Elastic Container Service com FSx o ONTAP
- Usando o Amazon Elastic VMware Service com o FSx ONTAP
- Usando o VMware Cloud com FSx for ONTAP

Usando a Amazon WorkSpaces com o FSx ONTAP

FSx for ONTAP pode ser usado com WorkSpaces a Amazon para fornecer armazenamento conectado à rede (NAS) compartilhado ou para armazenar perfis de roaming para contas da Amazon. WorkSpaces Depois de se conectar a um compartilhamento de arquivos SMB com uma WorkSpaces instância, o usuário pode criar e editar arquivos no compartilhamento de arquivos.

Os procedimentos a seguir mostram como usar a Amazon FSx com WorkSpaces a Amazon para fornecer ao perfil de roaming e ao acesso à pasta inicial uma experiência consistente e fornecer uma pasta de equipe compartilhada para WorkSpaces usuários de Windows e Linux. Se você é novo na

Amazon WorkSpaces, pode criar seu primeiro WorkSpaces ambiente Amazon com as instruções em Comece com a Configuração WorkSpaces Rápida no Guia de WorkSpaces Administração da Amazon.

Tópicos

- Fornecer suporte ao perfil de roaming
- Fornecer uma pasta compartilhada para acessar arquivos comuns

Fornecer suporte ao perfil de roaming

Você pode usar FSx a Amazon para fornecer suporte de perfil de roaming aos usuários da sua organização. Um usuário terá permissões para acessar somente seu perfil de roaming. A pasta será conectada automaticamente usando as políticas de grupo do Active Directory. Com um perfil de roaming, os dados e as configurações de desktop dos usuários são salvos quando eles se desconectam de um compartilhamento de FSx arquivos da Amazon, permitindo que documentos e configurações sejam compartilhados entre diferentes WorkSpaces instâncias, e o backup automático é feito automaticamente usando os backups automáticos FSx diários da Amazon.

Etapa 1: criar um local de pasta de perfil para usuários de domínio usando a Amazon FSx

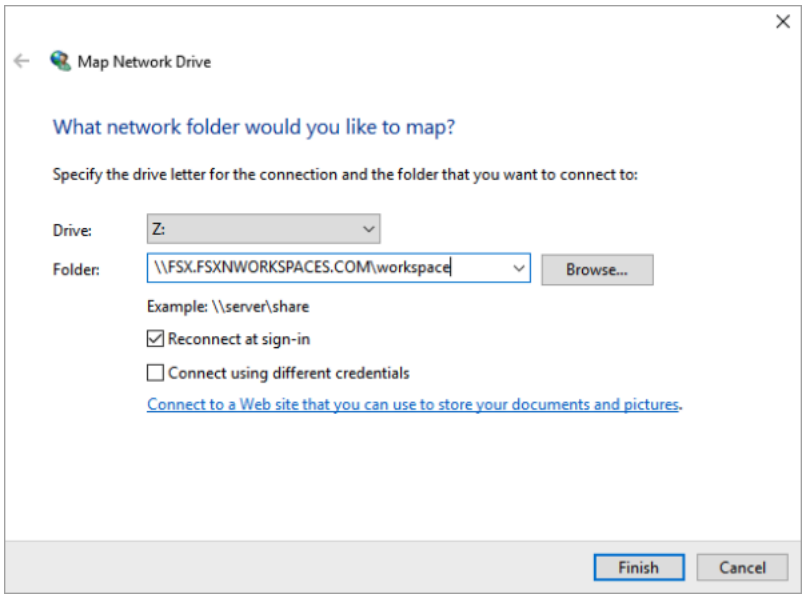
1. Crie um sistema de arquivos FSx for ONTAP usando o FSx console da Amazon. Para obter mais informações, consulte Criar um sistema de arquivos (console).

   > **Important**
   >
   > Cada sistema FSx de arquivos do ONTAP tem um intervalo de endereços IP de endpoint a partir do qual os endpoints associados ao sistema de arquivos são criados. Para sistemas de arquivos Multi-AZ, FSx o ONTAP escolhe um intervalo de endereços IP padrão não utilizado de 198.19.0.0/16 como o intervalo de endereços IP do endpoint. Esse intervalo de endereços IP também é usado WorkSpaces para gerenciar o intervalo de tráfego, conforme descrito nos requisitos de endereço IP e porta do Amazon WorkSpaces Administration Guide. WorkSpaces Como resultado, para acessar seu sistema de arquivos Multi-AZ FSx for ONTAP WorkSpaces, você deve selecionar um intervalo de endereços IP de endpoint que não se sobreponha ao 198.19.0.0/16.

2. Se você ainda não tiver uma máquina virtual de armazenamento (SVM) associada a um Active Directory, crie uma agora. Por exemplo, você pode provisionar uma SVM chamada `fsx` e definir

o estilo de segurança como NTFS. Para obter mais informações, consulte Criar uma máquina virtual de armazenamento (console).

3. Crie um volume para sua SVM. Por exemplo, você pode criar um volume chamado `fsx-vol` que herda o estilo de segurança do volume raiz da SVM. Para obter mais informações, consulte Para criar um FlexVol volume (console).
4. Crie um compartilhamento SMB em seu volume. Por exemplo, você pode criar um compartilhamento chamado `workspace` em seu volume chamado `fsx-vol`, no qual você cria uma pasta chamada `profiles`. Para obter mais informações, consulte Como gerenciar compartilhamentos de SMB.
5. Acesse seu Amazon FSx SVM a partir de uma EC2 instância da Amazon executando o Windows Server ou de um WorkSpace. Para obter mais informações, consulte Acessando seus dados FSx do ONTAP.
6. Você mapeia seu compartilhamento para `Z:\` na sua WorkSpaces instância do Windows:



Etapa 2: vincular o compartilhamento de arquivos FSx for ONTAP às contas de usuário

1. No seu usuário de teste WorkSpace, escolha Windows > Sistema > Configurações avançadas do sistema.
2. Em Propriedades do sistema, selecione a guia Avançado e pressione o botão Configurações na seção Perfis de usuário. O usuário conectado terá um tipo de perfil de `Local`.
3. Desconecte o usuário de teste do WorkSpace.

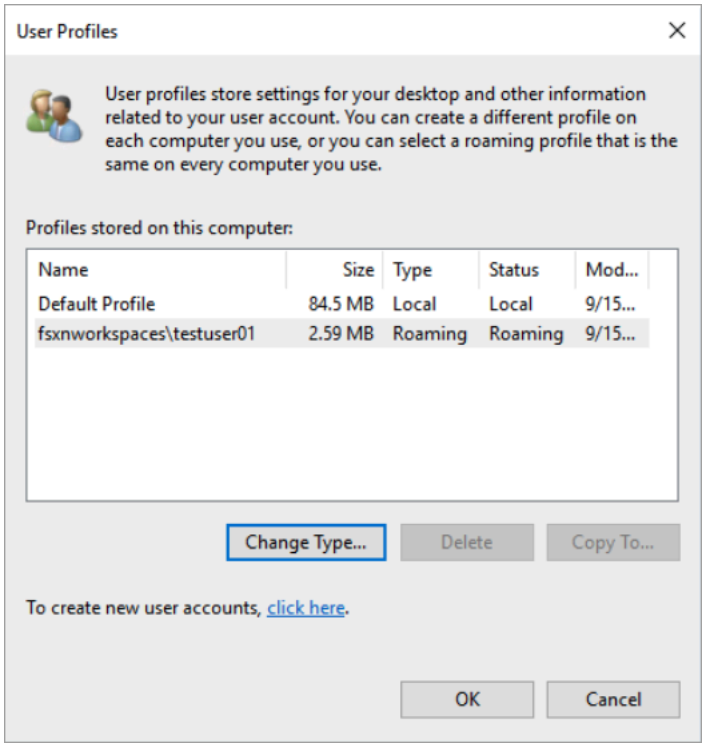
4. Configure o usuário de teste para ter um perfil de roaming localizado no seu sistema de FSx arquivos da Amazon. No seu administrador WorkSpaces, abra um PowerShell console e use um comando semelhante ao exemplo a seguir (que usa a `profiles` pasta que você criou anteriormente na Etapa 1):

```
Set-ADUser username -ProfilePath \\filesystem-dns-
name\sharename\foldername\username
```

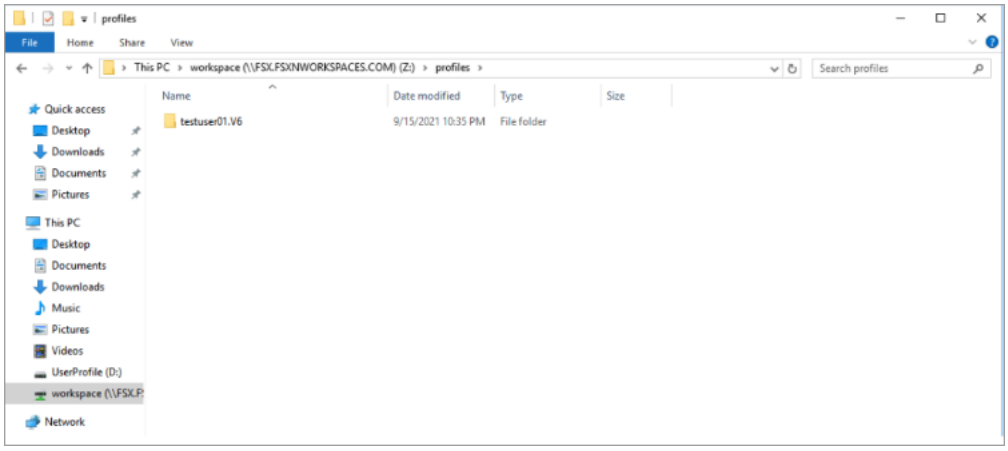
   Por exemplo:

```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxnworkspaces.com\workspace\profiles
\testuser01
```

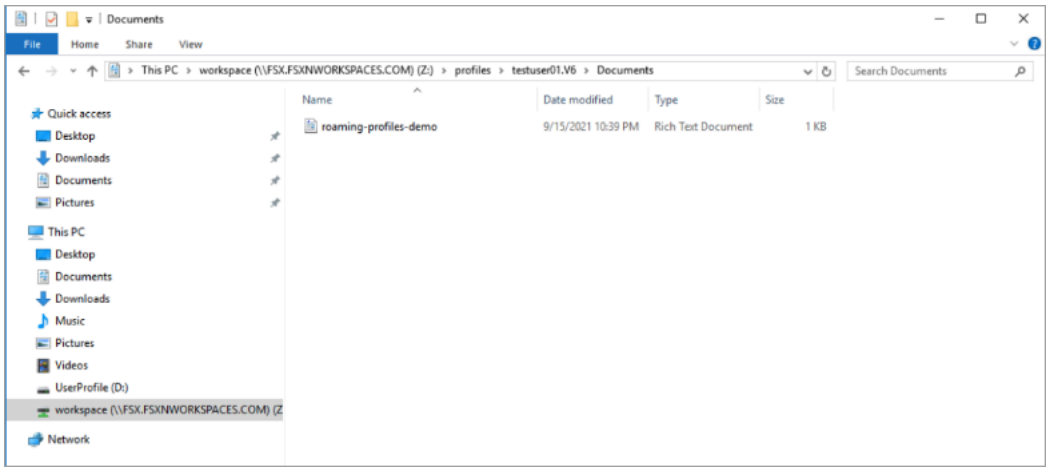
5. Faça login com o usuário de teste WorkSpace.
6. Em Propriedades do sistema, selecione a guia Avançado e pressione o botão Configurações na seção Perfis de usuário. O usuário conectado terá um tipo de perfil de `Roaming`.



7. FSx Procure a pasta compartilhada ONTAP. Na pasta `profiles`, você verá uma pasta para o usuário.



8. Criar um documento na pasta `Documents` do usuário de teste
9. Desconecte o usuário de teste do seu WorkSpace.
10. Se você se conectar novamente como usuário de teste e navegar até o armazenamento de perfis, verá o documento que criou.



Fornecer uma pasta compartilhada para acessar arquivos comuns

Você pode usar FSx a Amazon para fornecer uma pasta compartilhada aos usuários da sua organização. Uma pasta compartilhada pode ser usada para armazenar arquivos usados pela sua comunidade de usuários, como arquivos de demonstração, exemplos de código e manuais de instruções necessários para todos os usuários. Normalmente, você tem unidades mapeadas para pastas compartilhadas; no entanto, como as unidades mapeadas usam letras, há um limite para o número de compartilhamentos que você pode ter. Esse procedimento cria uma pasta FSx compartilhada da Amazon que está disponível sem uma carta de drive, oferecendo maior flexibilidade na atribuição de compartilhamentos às equipes.

Para montar uma pasta compartilhada para acesso multiplataforma a partir do Linux e do Windows WorkSpaces

1. Na barra de tarefas, escolha Locais > Conectar ao servidor.

   a. Em Servidor, insira*`file-system-dns-name`*.

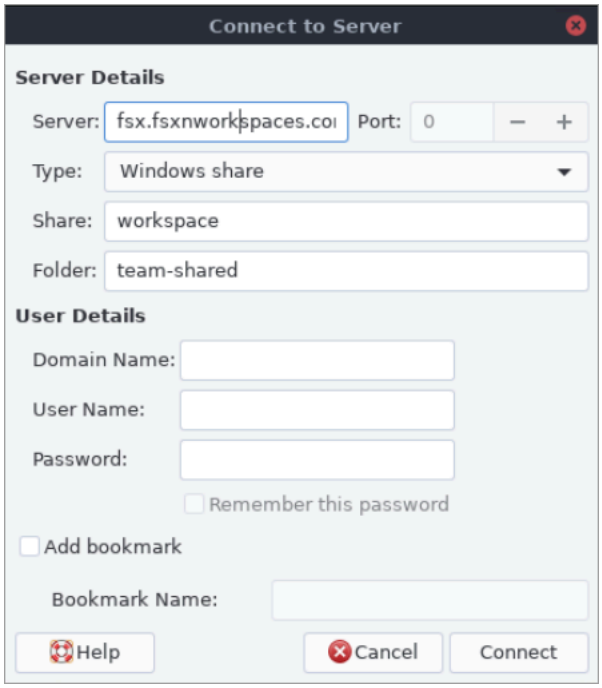
   b. Defina Tipo como `Windows share`.

   c. Defina Compartilhar para o nome do compartilhamento SMB, como `workspace`.

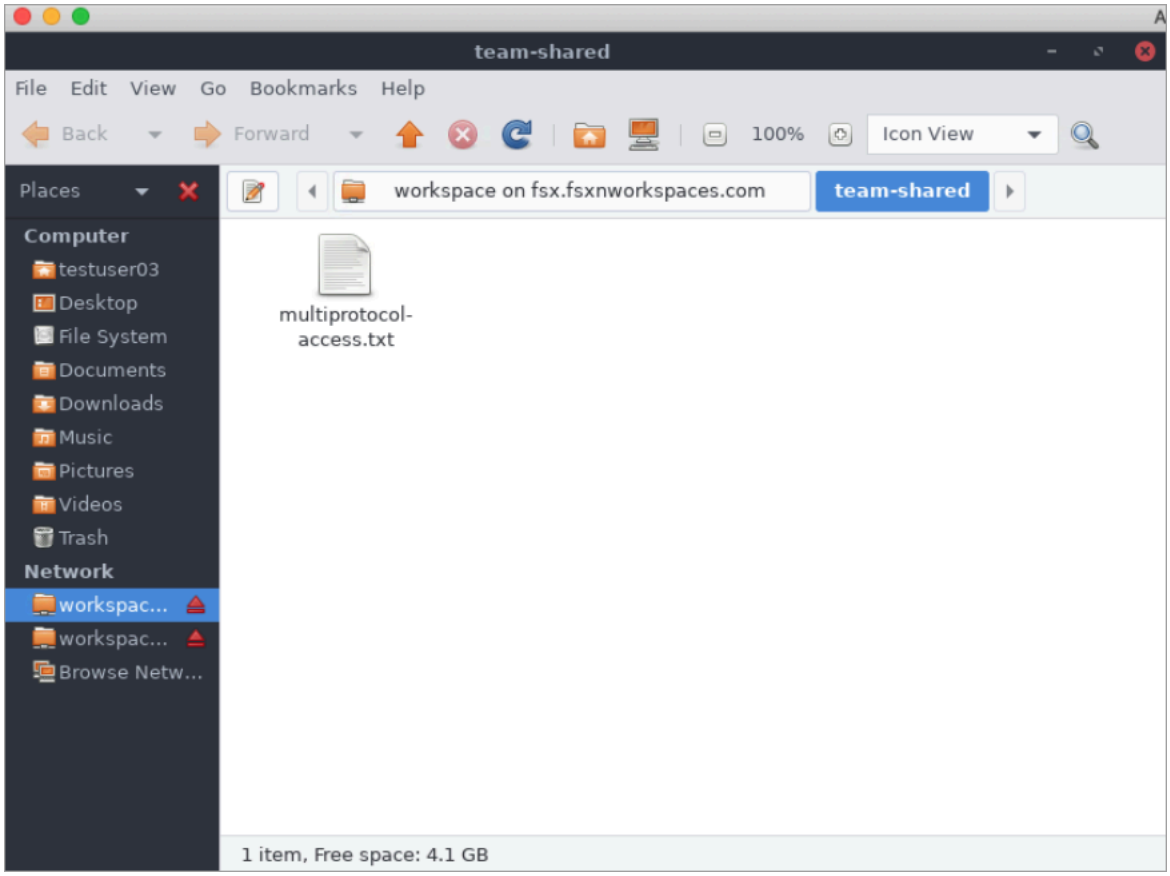
   d. Você pode deixar a Pasta como `/` ou defini-la como uma pasta, como uma pasta chamada `team-shared`.

   e. Para um Linux WorkSpace, você não precisa inserir seus detalhes de usuário se o Linux WorkSpace estiver no mesmo domínio do FSx compartilhamento da Amazon.

   f. Selecione Conectar.



2. Depois que a conexão for estabelecida, você poderá ver a pasta compartilhada (denominada `team-shared` neste exemplo) no compartilhamento SMB denominado `workspace`.



Usando o Amazon Elastic Container Service com FSx o ONTAP

Você pode acessar seus sistemas de arquivos Amazon FSx for NetApp ONTAP a partir de um contêiner Docker do Amazon Elastic Container Service (Amazon ECS) em uma instância do Amazon EC2 Linux ou Windows.

Montagem em um contêiner do Linux do Amazon ECS

1. Crie um cluster ECS usando o modelo de cluster EC2 Linux + Networking para seus contêineres Linux. Para obter mais informações, consulte Creating a cluster no Guia do desenvolvedor do Amazon Elastic Container Service.
2. Crie um diretório na EC2 instância para montar o volume SVM da seguinte forma:

```
sudo mkdir /fsxontap
```

3. Monte seu volume FSx for ONTAP na EC2 instância Linux usando um script de dados do usuário durante a execução da instância ou executando os seguintes comandos:

```
sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
```

4. Monte o volume usando o seguinte comando:

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /
fsxontap
```

O exemplo a seguir usa valores de amostra.

```
sudo mount -t nfs -o nfsvers=4.1
 svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
fsxontap
```

Você também pode usar o endereço IP da SVM em vez do nome DNS.

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. Ao criar suas definições de tarefas do Amazon ECS, adicione as propriedades de contêiner `volumes` e `mountPoints` a seguir na definição do contêiner JSON. `sourcePath`Substitua o pelo ponto de montagem e FSx pelo diretório em seu sistema de arquivos do ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Montagem em um contêiner do Windows do Amazon ECS

1. Crie um cluster ECS usando o modelo de cluster de rede EC2 do Windows + para seus contêineres do Windows. Para obter mais informações, consulte Creating a cluster no Guia do desenvolvedor do Amazon Elastic Container Service.
2. Adicione uma EC2 instância do Windows associada ao domínio ao cluster do ECS Windows e mapeie um compartilhamento SMB.

   Inicie uma EC2 instância do Windows otimizada para ECS que esteja associada ao seu domínio do Active Directory e inicialize o agente do ECS executando o comando a seguir.

   ```
   PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
   EnableTaskIAMRole
   ```

   Você também pode passar as informações em um script para o campo de texto de dados do usuário da forma a seguir.

   ```
   <powershell>
   Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
   </powershell>
   ```
3. Crie um mapeamento global SMB na EC2 instância para que você possa mapear seu compartilhamento SMB em uma unidade. Substitua os valores abaixo do nome netbios ou DNS do seu sistema de FSx arquivos e nome do compartilhamento. O volume NFS vol1 que foi montado na EC2 instância Linux está configurado como um compartilhamento CIFS fsxontap no sistema de arquivos. FSx

   ```
   vserver cifs share show -vserver svm08 -share-name fsxontap


                                   Vserver: svm08
                                     Share: fsxontap
                   CIFS Server NetBIOS Name: FSXONTAPDEMO
                                     Path: /vol1
                           Share Properties: oplocks
                                             browsable
                                             changenotify
                                             show-previous-versions
                         Symlink Properties: symlinks
                    File Mode Creation Mask: -
   ```

```
                 Directory Mode Creation Mask: -
                               Share Comment: -
                                   Share ACL: Everyone / Full Control
               File Attribute Cache Lifetime: -
                                 Volume Name: vol1
                               Offline Files: manual
           Vscan File-Operations Profile: standard
         Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -
```

4. Crie o mapeamento global SMB na EC2 instância usando o seguinte comando:

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. Ao criar suas definições de tarefas do Amazon ECS, adicione as propriedades de contêiner `volumes` e `mountPoints` a seguir na definição do contêiner JSON. `sourcePath`Substitua o pelo ponto de montagem e FSx pelo diretório em seu sistema de arquivos do ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Usando o Amazon Elastic VMware Service com o FSx ONTAP

Você pode usar o ONTAP como um armazenamento de dados externo FSx para os data centers definidos por software do Amazon Elastic Service VMware (Amazon EVS) (). SDDCs Para obter mais informações, consulte Executar cargas de trabalho de alto desempenho com a Amazon FSx para NetApp ONTAP. Para obter instruções detalhadas, consulte Configurar a Amazon FSx para NetApp ONTAP como um armazenamento de dados NFS e Configurar a Amazon FSx para NetApp ONTAP como um armazenamento de dados iSCSI.

Usando o VMware Cloud com FSx for ONTAP

Você pode usar o FSx ONTAP como um armazenamento de dados externo para o VMware Cloud on AWS Software-Defined Data Centers (). SDDCs Para obter mais informações, consulte Configurar o Amazon FSx para NetApp ONTAP como armazenamento externo e VMware Cloud on AWS with Amazon FSx for NetApp ONTAP Deployment Guide.

Opções de disponibilidade, durabilidade e implantação

O Amazon FSx for NetApp ONTAP usa os tipos de implantação Single-AZ e Multi-AZ. Você pode escolher entre quatro opções: Single-AZ 1, Single-AZ 2, Multi-AZ 1 e Multi-AZ 2. Este tópico descreve os recursos de disponibilidade e durabilidade de cada tipo de implantação para ajudar você a escolher o mais adequado às suas workloads. Para obter informações sobre o SLA (Service Level Agreement) de disponibilidade do serviço, consulte Amazon FSx Service Level Agreement.

Tópicos

- Escolher um tipo de implantação do sistema de arquivos
- Escolher uma geração de sistema de arquivos
- Processo de failover FSx para ONTAP
- Recursos da rede

Escolher um tipo de implantação do sistema de arquivos

Os recursos de disponibilidade e durabilidade dos tipos de implantação single-AZ e multi-AZ do sistema de arquivos são descritos nas seções a seguir.

Tipos de implantação Single-AZ

Você pode escolher entre Single-AZ 1 e Single-AZ 2 para seu sistema de arquivos Single-AZ. O Single-AZ 1 é um sistema de arquivos de primeira geração com um par de alta disponibilidade (HA), enquanto o Single-AZ 2 é um sistema de arquivos de segunda geração com 1 a 12 pares de HA. Para obter mais informações, consulte Escolher uma geração de sistema de arquivos.

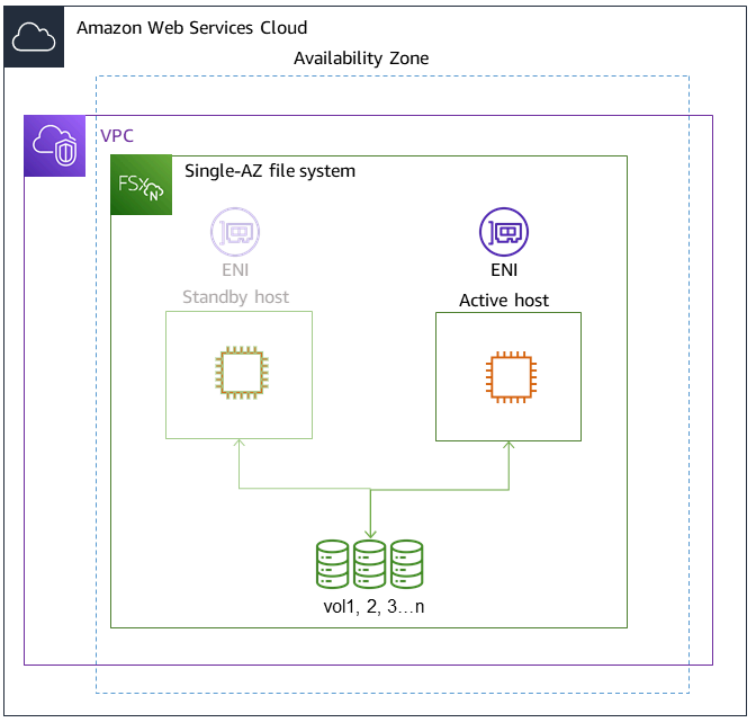
Quando você cria um sistema de arquivos Single-AZ, a Amazon provisiona FSx automaticamente de um a doze pares de servidores de arquivos em uma configuração ativa em espera, com os servidores de arquivos ativos e em espera em cada par localizados em domínios de falha separados em uma única zona de disponibilidade no. Região da AWS Durante a manutenção planejada do sistema de arquivos ou uma interrupção não planejada do serviço de qualquer servidor de arquivos ativo, a Amazon FSx transfere automaticamente e de forma independente esse par de alta disponibilidade (HA) para o servidor de arquivos em espera, normalmente em alguns segundos. Durante um failover, você continua a ter acesso aos seus dados sem intervenção manual.

Para garantir a alta disponibilidade, a Amazon monitora FSx continuamente as falhas de hardware e substitui automaticamente os componentes da infraestrutura em caso de falha. Para obter

alta durabilidade, a Amazon replica FSx automaticamente seus dados dentro de uma zona de disponibilidade para protegê-los contra falhas de componentes. Além disso, você tem a opção de configurar backups diários automáticos dos dados do sistema de arquivos. Esses backups são armazenados em várias zonas de disponibilidade para fornecer resiliência multi-AZ a todos os dados de backup.

Os sistemas de arquivos single-AZ são projetados para casos de uso que não exigem o modelo de resiliência de dados de um sistema de arquivos multi-AZ. Eles fornecem uma solução econômica para casos de uso, como ambientes de desenvolvimento e teste, ou armazenamento de cópias secundárias de dados que já estão armazenados no local ou em outros ambientes Regiões da AWS, replicando dados somente em uma única zona de disponibilidade.

O diagrama a seguir ilustra a arquitetura de um sistema de arquivos FSx de primeira geração ONTAP Single-AZ.

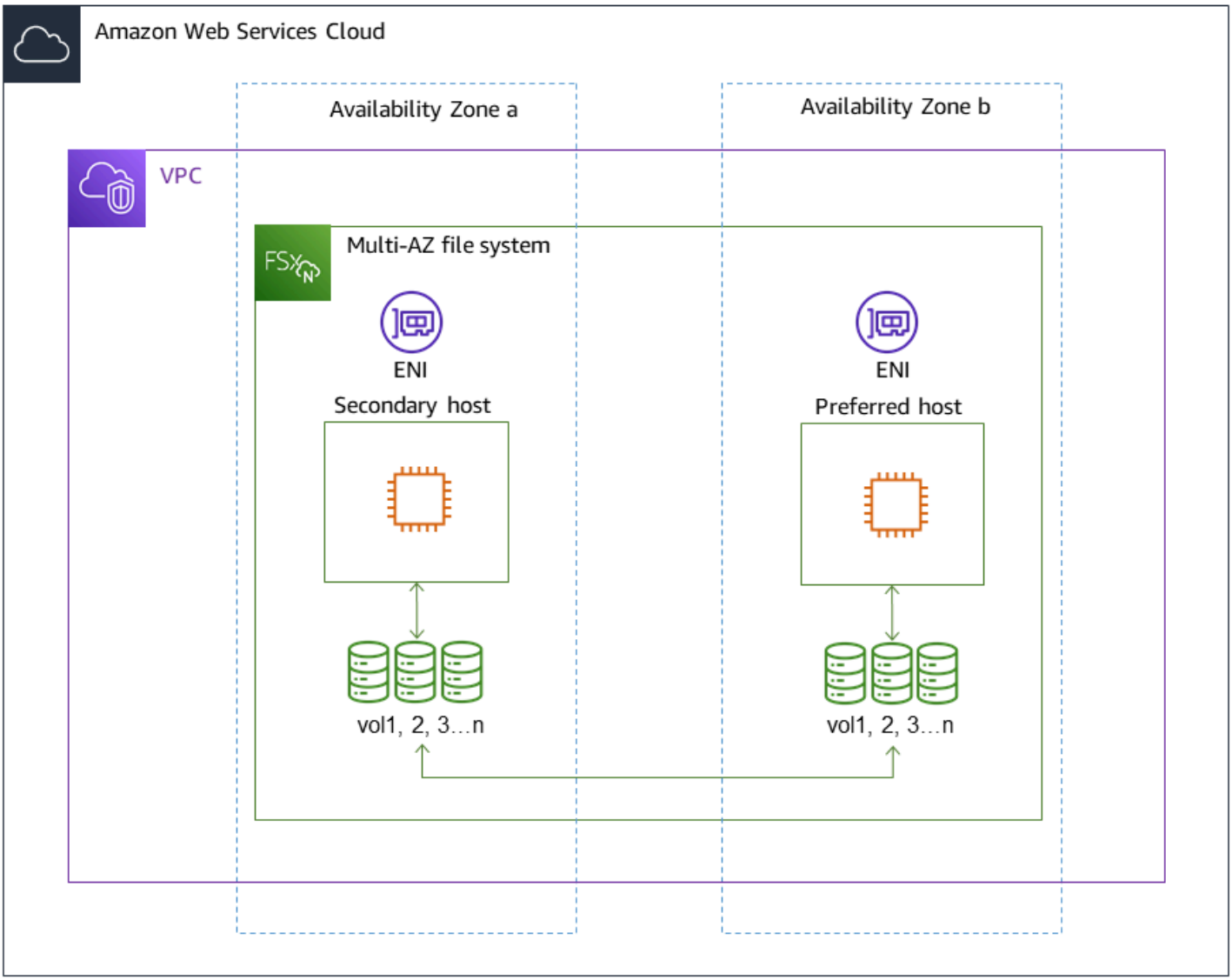


Tipos de implantação Multi-AZ

Você pode escolher entre Multi-AZ 1 e Multi-AZ 2 para seu sistema de arquivos Multi-AZ. O Multi-AZ 1 é um sistema de arquivos de primeira geração e o Multi-AZ 2 é um sistema de arquivos de segunda geração. Ambas as opções têm um par de HA. Para obter mais informações, consulte Escolher uma geração de sistema de arquivos.

Os sistemas de arquivos multi-AZ oferecem suporte a todos os recursos de disponibilidade e durabilidade dos sistemas de arquivos single-AZ. Além disso, eles são projetados para fornecer disponibilidade contínua aos dados, mesmo quando uma zona de disponibilidade não estiver disponível. As implantações Multi-AZ têm um único par de HA de servidores de arquivos, com o servidor de arquivos em espera implantado em uma zona de disponibilidade diferente do servidor de arquivos ativo na mesma Região da AWS. Todas as alterações gravadas no sistema de arquivos são replicadas de forma síncrona nas zonas de disponibilidade para o modo de espera.

Os sistemas de arquivos multi-AZ são projetados para casos de uso, como workloads de produção essenciais para os negócios, que exigem alta disponibilidade para dados de arquivos compartilhados do ONTAP e precisam de armazenamento com replicação integrada em todas as zonas de disponibilidade. O diagrama a seguir ilustra a arquitetura de um sistema de arquivos de primeira FSx geração para ONTAP Multi-AZ.



Escolher uma geração de sistema de arquivos

A tabela a seguir ilustra as diferenças entre Single-AZ e Multi-AZ de primeira e segunda geração FSx para sistemas de arquivos ONTAP.

FSx para gerações de sistemas de arquivos ONTAP

Dimensão	Primeira geração	Segunda geração (par único de HA)	Segunda geração (vários pares)
Tipo de implantação	SINGLE_AZ_1 MULTI_AZ_1	SINGLE_AZ_2 MULTI_AZ_2	SINGLE_AZ_2
Pares de HA	1 par de HA		1 a 12 pares de HA
Armazenamento em SSD	Mínimo: 1 TiB Máximo: 192 TiB	Mínimo: 1 TiB Máximo: 512 TiB	Mínimo: 1 TiB (por par de HA) Máximo: 1 PiB (total)
IOPS SSD	Mínimo: 3 IOPS/ GIB de SSD Máximo: 160.000	Mínimo: 3 IOPS/ GIB de SSD Máximo: 200.000	Mínimo: 3 IOPS/ GIB de SSD Máximo: 2.400.000 (200.000 por par de HA)
Capacidade de throughput	128 MBps; 256; 512 MBps; 1.024 MBps; 2.048 MBps; 4.096 MBps MBps	384 MBps; 768; 1.536 MBps MBps; 3.072; 6.144 MBps MBps	1.536 MBps (por par de HA); 3.072 MBps (por par de HA); 6.144 MBps (por par de HA)

> **Note**
>
> Você não pode alterar o tipo de implantação do sistema de arquivos após a criação. Se quiser alterar o tipo de implantação (por exemplo, passar da Single-AZ 1 para a Single-AZ 2), você poderá fazer backup dos dados e restaurá-los em um novo sistema de arquivos. Você também pode migrar seus dados com NetApp SnapMirror AWS DataSync, com ou com uma

ferramenta de cópia de dados de terceiros. Para ter mais informações, consulte Migrando FSx para o ONTAP usando NetApp SnapMirror e Migrando FSx para o ONTAP usando AWS DataSync.

Processo de failover FSx para ONTAP

No caso de ocorrência de alguma das seguintes condições, os sistemas de arquivos Single-AZ e Multi-AZ farão o failover automático de um determinado par de HA do servidor de arquivos preferencial ou ativo para o servidor de arquivos em espera:

- O servidor de arquivos preferencial ou ativo fica indisponível
- A capacidade de throughput do sistema de arquivos é alterada
- O servidor de arquivos preferencial ou ativo passa por uma manutenção planejada
- Ocorre uma interrupção na zona de disponibilidade (somente sistemas de arquivos multi-AZ)

> **Note**
>
> Para sistemas de arquivos de segunda geração com vários pares de HA, o comportamento de failover de cada par de HA é independente. Se o servidor de arquivos preferencial para um par de HA não estiver disponível, somente esse par de HA fará o failover para seu servidor de arquivos em espera.

Ao fazer o failover de um servidor de arquivos para outro, o novo servidor de arquivos ativo começará automaticamente a atender a todas as solicitações de leitura e gravação do sistema de arquivos do respectivo par de HA. Para sistemas de arquivos Multi-AZ, quando o servidor de arquivos preferido é totalmente recuperado e fica disponível, a Amazon retorna FSx automaticamente a ele, com o failback geralmente concluído em menos de 60 segundos. Para sistemas de arquivos single-AZ e multi-AZ, um failover geralmente é concluído em menos de 60 segundos, desde a detecção da falha no servidor de arquivos ativo até a promoção do servidor de arquivos em espera para o status ativo. Como o endereço IP do endpoint que os clientes usam para acessar dados por NFS ou SMB permanece o mesmo, os failovers são transparentes para aplicações do Linux, Windows e macOS, que retomam as operações do sistema de arquivos sem intervenção manual.

Para garantir que os failovers sejam transparentes para os clientes conectados aos seus FSx sistemas de arquivos ONTAP Single-AZ e Multi-AZ, consulte. Acessando dados de dentro do Nuvem AWS

Como testar o failover em um sistema de arquivos

Você pode testar o failover no sistema de arquivos modificando sua capacidade de throughput. Quando você modifica a capacidade de taxa de transferência do seu sistema de arquivos, a Amazon FSx desativa os servidores de arquivos do sistema de arquivos em série. Os sistemas de arquivos passam automaticamente para o servidor secundário, enquanto a Amazon FSx substitui primeiro o servidor de arquivos preferencial. Depois de atualizado, o sistema de arquivos retorna automaticamente para o novo servidor primário e a Amazon FSx substitui o servidor de arquivos secundário.

Você pode monitorar o progresso da solicitação de atualização da capacidade de transferência no FSx console da Amazon, na CLI e na API. Para obter mais informações sobre como modificar a capacidade de throughput do sistema de arquivos e monitorar o progresso da solicitação, consulte Como gerenciar a capacidade de throughput.

Recursos da rede

Esta seção descreve os recursos de rede consumidos pelos sistemas de arquivos single-AZ e multi-AZ.

Sub-redes

Ao criar um sistema de arquivos single-AZ, você especifica uma única sub-rede para o sistema de arquivos. A sub-rede escolhida define a zona de disponibilidade na qual o sistema de arquivos é criado. Ao criar um sistema de arquivos multi-AZ, você especifica duas sub-redes, uma para o servidor de arquivos preferencial e outra para o servidor de arquivos em espera. As duas sub-redes escolhidas devem estar em zonas de disponibilidade diferentes na mesma Região da AWS. Para obter mais informações sobre a Amazon VPC, consulte O que é Amazon VPC? no Guia do usuário da Amazon Virtual Private Cloud.

> **Note**
>
> Independentemente da sub-rede especificada, você pode acessar seu sistema de arquivos de qualquer sub-rede dentro da VPC do sistema de arquivos.

Interfaces de rede elástica do sistema de arquivos

Para sistemas de arquivos Single-AZ, a Amazon FSx provisiona duas interfaces de rede elásticas (ENI) na sub-rede que você associa ao seu sistema de arquivos. Para sistemas de arquivos Multi-AZ, a Amazon FSx também provisiona dois ENIs, um em cada uma das sub-redes que você associa ao seu sistema de arquivos. Os clientes se comunicam com seu sistema de FSx arquivos da Amazon usando a interface de rede elástica. As interfaces de rede são consideradas dentro do escopo de serviço da Amazon FSx, apesar de fazerem parte da VPC da sua conta. Os sistemas de arquivos Multi-AZ usam endereços IP flutuantes para que os clientes conectados façam uma transição perfeita entre os servidores de arquivos preferencial e de espera durante um evento de failover.

> ⚠ Warning
>
> - Você não deve modificar ou excluir as interfaces de rede elástica associadas ao seu sistema de arquivos. A modificação ou a exclusão da interface de rede pode causar uma perda permanente de conexão entre a VPC e o sistema de arquivos.
> - As interfaces de rede elástica associadas ao sistema de arquivos terão rotas criadas automaticamente e adicionadas às tabelas de rotas da sub-rede e da VPC padrão. Modificar ou excluir essas rotas pode causar perda temporária ou permanente de conectividade para os clientes do sistema de arquivos.

A tabela a seguir resume os recursos de sub-rede, elastic network interface e endereço IP para cada um dos tipos de implantação do FSx sistema de arquivos ONTAP:

	Single-AZ de primeira geração	Single-AZ de segunda geração	Multi-AZ
Número de sub-redes	1	1	2
Número de interfaces de rede elástica	2	2 por par de HA	2

	Single-AZ de primeira geração	Single-AZ de segunda geração	Multi-AZ
Número de endereços IP por ENI	1 + o número de SVMs no sistema de arquivos	Contagem de pares HA + contagem de pares HA multiplicada pelo número de SVMs no sistema de arquivos	1 + o número de SVMs no sistema de arquivos
Número de rotas da tabela de rotas da VPC	N/D	N/D	1 + o número de SVMs no sistema de arquivos

Depois que um sistema de arquivos ou uma SVM são criados, os endereços IP não mudam até que o sistema de arquivos seja excluído.

> **Important**
>
> A Amazon FSx não oferece suporte para acessar sistemas de arquivos nem expor sistemas de arquivos à Internet pública. A Amazon separa FSx automaticamente qualquer endereço IP elástico, que é um endereço IP público acessível pela Internet, que é anexado à interface de rede elástica de um sistema de arquivos.

Amazon FSx para desempenho do NetApp ONTAP

Veja a seguir uma visão geral do desempenho do sistema de arquivos Amazon FSx for NetApp ONTAP, com uma discussão sobre as opções disponíveis de desempenho e taxa de transferência e dicas úteis de desempenho.

Tópicos

- Como o desempenho é medido FSx para sistemas de arquivos ONTAP
- Detalhes da performance
- Impacto do tipo de implantação na performance
- Impacto da capacidade de armazenamento na performance
- Impacto da capacidade de throughput na performance
- Exemplo: capacidade de armazenamento e capacidade de throughput

Como o desempenho é medido FSx para sistemas de arquivos ONTAP

O desempenho do sistema de arquivos é medido por sua latência, taxa de transferência e I/O operações por segundo (IOPS).

Latência

O Amazon FSx for NetApp ONTAP fornece latências de operação de arquivos abaixo de um milissegundo com armazenamento em unidade de estado sólido (SSD) e dezenas de milissegundos de latência para armazenamento em pool de capacidade. Além disso, a Amazon FSx tem duas camadas de cache de leitura em cada servidor de arquivos — unidades NVMe (memória expressa não volátil) e na memória — para fornecer latências ainda mais baixas quando você acessa seus dados lidos com mais frequência.

Throughput e IOPS

Cada sistema de FSx arquivos da Amazon fornece até dezenas de taxa GBps de transferência e milhões de IOPS. A quantidade específica de throughput e IOPS que sua workload pode gerar no sistema de arquivos depende da capacidade de throughput total e da configuração da capacidade

de armazenamento do sistema de arquivos, com a natureza da workload, incluindo o tamanho do conjunto de trabalho ativo.

Suporte para SMB Multichannel e NFS nconnect

Com a Amazon FSx, você pode configurar o SMB Multichannel para fornecer várias conexões entre ONTAP e clientes em uma única sessão SMB. O SMB Multichannel usa várias conexões de rede entre o cliente e o servidor simultaneamente para agregar largura de banda da rede para a máxima utilização. Para obter informações sobre como usar a CLI do NetApp ONTAP para configurar o SMB Multichannel, consulte Configuring SMB Multichannel for performance and redundancy.

Os clientes NFS podem usar a opção de montagem `nconnect` para ter várias conexões TCP (até 16) associadas a uma única montagem NFS. Esse cliente NFS multiplexa as operações de arquivo em várias conexões TCP de forma round-robin e, assim, obtém maior taxa de transferência da largura de banda de rede disponível. NFSv3 e suporte NFSv4 1.1 ou superior. `nconnect` A largura de banda de rede da EC2 instância Amazon descreve o limite de largura de banda full duplex de 5 Gbps por fluxo de rede. Você pode superar esse limite usando vários fluxos de rede com `nconnect` ou SMB Multichannel. Consulte a documentação do seu cliente NFS para confirmar se há suporte para `nconnect` na versão do cliente. Para obter mais informações sobre NetApp ONTAP suporte para`nconnect`, consulte ONTAPsuporte para NFSv4 .1.

Quadros Jumbo

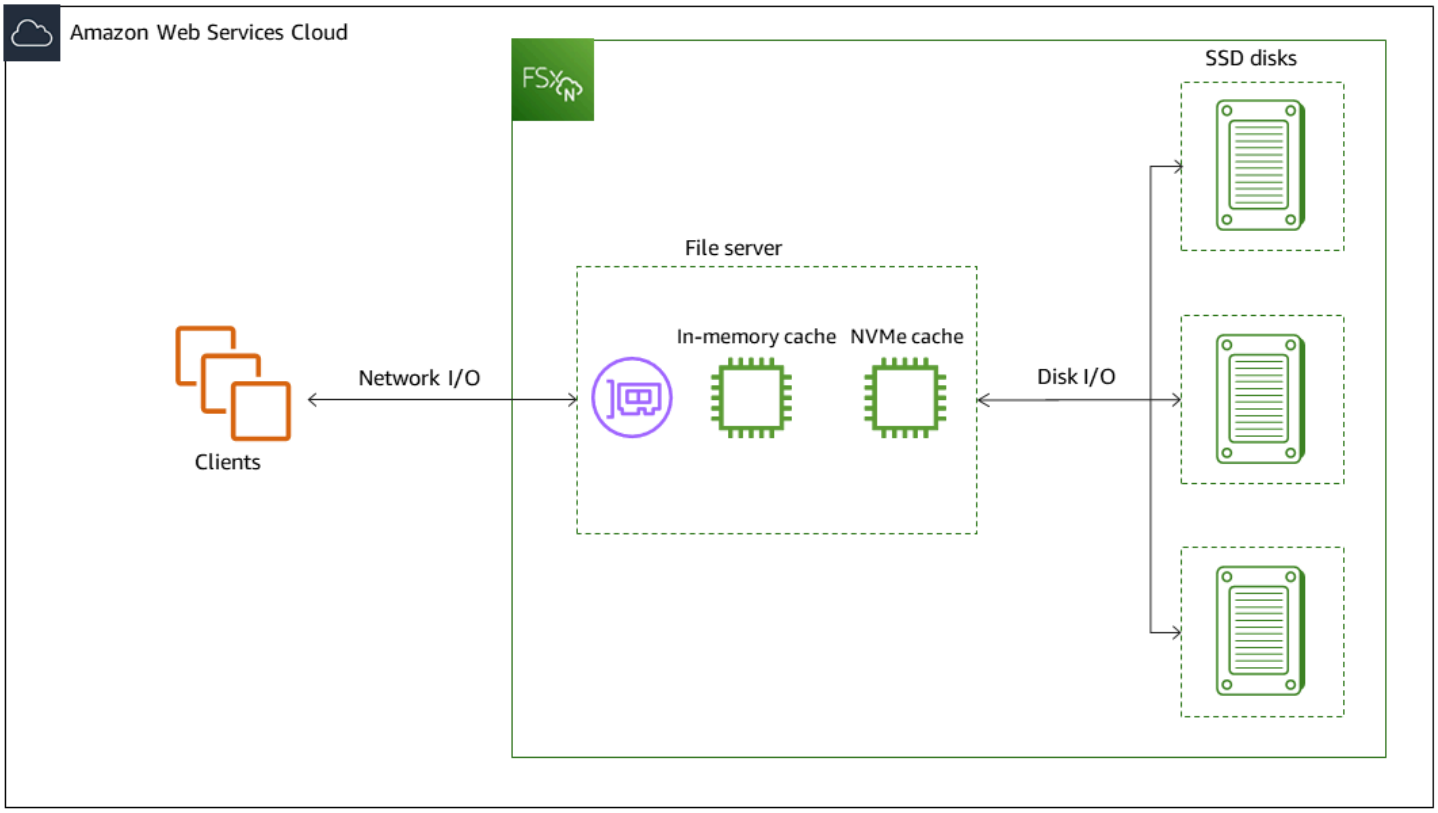
Para obter a máxima taxa de transferência de leitura ou gravação, recomendamos habilitar jumbo frames em todas as interfaces de rede no caminho de dados para o sistema de FSx arquivos da Amazon, incluindo as instâncias do cliente EC2 . A configuração padrão da unidade máxima de transmissão (MTU) para interfaces de rede em seu sistema de arquivos FSx for ONTAP é 9.001 bytes.

Detalhes da performance

Para entender detalhadamente o modelo de desempenho do Amazon FSx for NetApp ONTAP, você pode examinar os componentes arquitetônicos de um sistema de FSx arquivos da Amazon. Suas instâncias de computação cliente, estejam elas no local AWS ou no local, acessam seu sistema de arquivos por meio de uma ou várias interfaces de rede elástica (ENI). Essas interfaces de rede residem na Amazon VPC associada ao seu sistema de arquivos. Por trás de cada ENI do sistema de arquivos está um servidor de arquivos do NetApp ONTAP que fornece dados pela rede aos clientes que acessam o sistema de arquivos. FSxA Amazon fornece um cache rápido na memória e um

NVMe cache em cada servidor de arquivos para melhorar o desempenho dos dados acessados com mais frequência. Os discos SSD que hospedam os dados do sistema de arquivos estão anexados a cada servidor de arquivos.

Esses componentes são ilustrados no diagrama a seguir.



Correspondendo a esses componentes arquitetônicos — interface de rede, cache na memória, NVMe cache e volumes de armazenamento — estão as principais características de desempenho de um sistema de arquivos Amazon FSx for NetApp ONTAP que determinam a taxa de transferência geral e o desempenho de IOPS.

- I/O Desempenho da rede: throughput/IOPS de solicitações entre os clientes e o servidor de arquivos (em conjunto)
- Tamanho da memória e do NVMe cache no servidor de arquivos: tamanho do conjunto de trabalho ativo que pode ser acomodado para armazenamento em cache
- I/O Desempenho do disco: throughput/IOPS de solicitações entre o servidor de arquivos e os discos de armazenamento

Há dois fatores que determinam essas características de desempenho no sistema de arquivos: a quantidade total de IOPS de SSD e a capacidade de throughput configurada para ele. As duas

primeiras características de desempenho — I/O desempenho da rede e tamanho da memória e do NVMe cache — são determinadas exclusivamente pela capacidade de taxa de transferência, enquanto a terceira — desempenho de E/S de disco — é determinada por uma combinação de capacidade de taxa de transferência e IOPS de SSD.

As cargas de trabalho baseadas em arquivos geralmente apresentam picos, caracterizados por períodos curtos e intensos de alta temperatura, I/O com bastante tempo ocioso entre as rajadas. Para suportar cargas de trabalho com picos, além das velocidades básicas que um sistema de arquivos pode sustentar 24 horas por dia, 7 dias por semana, a Amazon FSx oferece a capacidade de atingir velocidades mais altas por períodos de tempo, tanto para operações de rede quanto de disco. I/O I/O A Amazon FSx usa um mecanismo I/O de crédito de rede para alocar a taxa de transferência e o IOPS com base na utilização média — os sistemas de arquivos acumulam créditos quando a taxa de transferência e o uso de IOPS estão abaixo dos limites básicos e podem usar esses créditos ao realizar operações. I/O

> **Note**
>
> Para os protocolos iSCSI e NVMe/TCP SAN, as operações de leitura sequencial do cliente podem atingir até a máxima I/O intermitência de rede ou a taxa de transferência básica do sistema de arquivos.

As operações de gravação usam duas vezes mais largura de banda da rede do que as operações de leitura. Uma operação de gravação precisa ser replicada no servidor de arquivos secundário. Portanto, uma única operação de gravação resulta no dobro de throughput de rede.

Impacto do tipo de implantação na performance

Você pode criar sistemas de arquivos Single-AZ e Multi-AZ com o FSx for ONTAP. Os sistemas de arquivos de primeira geração (Single-AZ e Multi-AZ) e os sistemas de arquivos Multi-AZ de segunda geração são alimentados por um par de alta disponibilidade (HA). Os sistemas de arquivos Single-AZ de segunda geração são habilitados por até 12 pares de HA. Para obter mais informações, consulte Gerenciar pares de alta disponibilidade (HA).

FSx para sistemas de arquivos ONTAP Multi-AZ e Single-AZ, fornecem latências consistentes de operação de arquivos abaixo de um milissegundo com armazenamento SSD e dezenas de milissegundos de latência com armazenamento em pool de capacidade. Além disso, os sistemas de

arquivos que atendem aos requisitos a seguir fornecem um cache de NVMe leitura para reduzir as latências de leitura e aumentar o IOPS para dados lidos com frequência:

- Sistemas de arquivos Multi-AZ 1 e Multi-AZ 2
- Sistemas de arquivos Single-AZ 1 criados após 28 de novembro de 2022 com pelo menos 2% GBps da capacidade de taxa de transferência
- Sistemas de arquivos Single-AZ 2 com pelo menos 6% GBps da capacidade de taxa de transferência por par

> **Note**
>
> Para sistemas de arquivos de segunda geração (Single-AZ 2 e Multi-AZ 2), o uso de um NVMe cache pode fazer com que sua carga de trabalho alcance menos taxa de transferência total para cargas de trabalho de E/S de alto rendimento ou grandes. Se você tiver uma carga de trabalho limitada à taxa de transferência, recomendamos desativar o cache. NVMe Para obter mais informações, consulte Gerenciando o NVMe cache.

As tabelas a seguir mostram a quantidade de capacidade de throughput que os sistemas de arquivos podem atingir, dependendo de fatores como o número de pares de alta disponibilidade (HA) e a Regiões da AWS disponibilidade.

First-generation file systems

Essas especificações de desempenho se aplicam aos sistemas de arquivos Single-AZ e Multi-AZ de primeira geração.

Throughput máximo do armazenamento SSD por par de HA para sistemas de arquivos de primeira geração

Regiões Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda)		Todos os outros Regiões da AWS locais onde FSx o ONTAP está disponível	
Taxa de transferência	Taxa de transferência	Taxa de transferência	Taxa de transferência

	Regiões Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda)		Todos os outros Regiões da AWS locais onde FSx o ONTAP está disponível	
	de leitura () MBps	de gravação () MBps	de leitura () MBps	de gravação () MBps
Single-AZ	4.096 [1]	1.000	2.048	750
Multi-AZ	4.096 [1]	1,800	2.048	1.300

> **Note**
>
> [1] Para provisionar 4% GBps da capacidade de taxa de transferência, seu sistema de arquivos deve ser configurado com um mínimo de 5.120 GiB de capacidade de armazenamento SSD e 160.000 SSD IOPS.

Second-generation file systems

Essas especificações de desempenho se aplicam aos sistemas de arquivos Single-AZ e Multi-AZ de segunda geração. Geralmente, os sistemas de arquivos de segunda geração podem fornecer a capacidade total provisionada para leituras e até um terço da capacidade de throughput provisionada para gravações. A exceção é a MB/s opção 6.144, listada nesta tabela.

Throughput máximo do armazenamento SSD por par de HA para sistemas de arquivos de segunda geração

	Taxa de transferência de leitura () MBps	Taxa de transferência de gravação () MBps
Single-AZ	6.144 [1]	1.024 [1]
Multi-AZ	6,144	2.048

> **Note**
>
> [1] por par de HA (até 12). Para obter mais informações, consulte Gerenciar pares de alta disponibilidade (HA).

Impacto da capacidade de armazenamento na performance

O throughput máximo de disco e os níveis de IOPS que o sistema de arquivos pode alcançar são os mais baixos entre:

- o nível de desempenho do disco fornecido pelos servidores de arquivos, com base na capacidade de throughput selecionada para o sistema de arquivos
- o nível de performance do disco fornecido pelo número de IOPS de SSD provisionado para o sistema de arquivos

Por padrão, o armazenamento SSD do sistema de arquivos fornece até os seguintes níveis de throughput de disco e IOPS:

- Taxa de transferência de disco (MBps por TiB de armazenamento): 768
- IOPS de disco (IOPs por TiB de armazenamento): 3.072

Impacto da capacidade de throughput na performance

Cada sistema de FSx arquivos da Amazon tem uma capacidade de taxa de transferência que você configura quando o sistema de arquivos é criado. A capacidade de taxa de transferência do seu sistema de arquivos determina o nível de I/O desempenho da rede ou a velocidade com que cada um dos servidores de arquivos que hospedam seu sistema de arquivos pode fornecer dados de arquivos pela rede aos clientes que os acessam. Níveis mais altos de capacidade de taxa de transferência vêm com mais memória e armazenamento não volátil de memória express (NVMe) para armazenar dados em cache em cada servidor de arquivos e níveis mais altos de I/O desempenho de disco suportados por cada servidor de arquivos.

Opcionalmente, você pode provisionar um nível mais alto de IOPS de SSD ao criar o sistema de arquivos. O nível máximo de IOPS de SSD que o sistema de arquivos pode alcançar também é

determinado pela capacidade de throughput do sistema de arquivos, mesmo ao provisionar IOPS de SSD adicionais.

As tabelas a seguir mostram o conjunto completo de especificações de capacidade de throughput, com os níveis de linha de base e de intermitência e a quantidade de memória para armazenamento em cache no servidor de arquivos nas Regiões da AWS correspondentes.

First-generation Single-AZ file system

Essas especificações de desempenho se aplicam aos sistemas de arquivos Single-AZ de primeira geração criados após 28 de novembro de 2022 nas Regiões da AWS especificadas.

Especificações de desempenho para sistemas de arquivos nos seguintes Regiões da AWS: Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon) e Europa (Irlanda)

FSxcapacidade de produção () MBps	Capacidade de taxa de transferência da rede () MBps		IOPS de rede	Armazenamento em cache na memória (GB)	NVMe cache de leitura (GB)	Taxa de transferência de disco () MBps		IOPS de unidade SSD *	
	Linha de base	Intermitência				Linha de base	Intermitência	Linha de base	Intermitência
128	188	1.500	Linha de base de dezenas de milhares	16	–	128	1.250	6.000	40.000
256	375	1.500		32	–	256	1.250	12.000	40.000
512	750	1.500		64	–	512	1.250	20.000	40.000
1,024	1.500	–		128	–	1,024	1.250	40.000	–
2.048	3.125	–		256	1.900	2.048	–	80.000	–

FSxcapacidade de produção () MBps	Capacidade de taxa de transferência da rede () MBps		IOPS de rede	Armazenamento em cache na memória (GB)	NVMe cache de leitura (GB)	Taxa de transferência de disco () MBps		IOPS de unidade SSD *	
4.096	6.250	–	centenas de milhares	512	5.400	4.096	–	160.000	–

> **Note**
>
> * Seu SSD IOPS só é usado quando você acessa dados que não estão em cache no cache ou cache na memória do seu servidor de arquivos. NVMe

Essas especificações de desempenho se aplicam aos sistemas de arquivos Single-AZ de primeira geração em todos os outros Regiões da AWS lugares FSx em que o ONTAP está disponível.

Especificações de desempenho para sistemas de arquivos em [todos os outros Regiões da AWS lugares onde FSx o ONTAP está disponível]

FSx capacidade de produção () MBps	Capacidade de taxa de transferência da rede () MBps		IOPS de rede	Armazenamento em cache na memória (GB)	Taxa de transferência de disco () MBps		IOPS de unidade SSD *	
	Linha de base	Intermitência			Linha de base	Intermitência	Linha de base	Intermitência
128	150	1.250	Linha de	16	128	600	6.000	18.750

FSx capacidade de produção () MBps	Capacidade de taxa de transferência da rede () MBps		IOPS de rede	Armazenamento em cache na memória (GB)	Taxa de transferência de disco () MBps		IOPS de unidade SSD *	
256	300	1.250	base de dezenas de milhares	32	256	600	12.000	18.750
512	625	1.250	Linha de base de centenas de milhares	64	512	600	18.750	–
1,024	1.500	–		128	1,024	–	40.000	–
2.048	3.125	–		256	2.048	–	80.000	–

> **Note**
>
> * Seu SSD IOPS só é usado quando você acessa dados que não estão em cache no cache ou cache na memória do seu servidor de arquivos. NVMe

Second-generation Single-AZ file system

Essas especificações de desempenho se aplicam aos sistemas de arquivos Single-AZ de segunda geração.

Especificações de desempenho dos sistemas de arquivos Single-AZ de segunda geração

FSx capacidade de produção () MBps	Capacidade de taxa de transferência da rede () MBps		IOPS de rede	Armazenamento em cache na memória (GB)	NVMe armazenamento em cache (GB)	Taxa de transferência de disco () MBps		IOPS de unidade SSD *	
	Linha de base	Intermitência				Linha de base	Intermitência	Linha de base	Intermitência
384**	781	6.250	Linha de base de centenas de milhares	16	–	384	3.125	12.500	65.000
768**	1.563	6.250		32	–	768	3.125	25.000	65.000
1.536	3.125	6.250		64	–	1.536	3.125	50.000	65.000
3.072	6.250	–		128	–	3.072	–	100.000	–
6,144	12.500	–		256	1.900	6,144	–	200.000	–

> **Note**
>
> * Seu SSD IOPS só é usado quando você acessa dados que não estão em cache no cache ou cache na memória do seu servidor de arquivos. NVMe
> ** Os sistemas de arquivos Single-AZ de segunda geração são compatíveis com as capacidades de throughput de 384 e 768, mas somente com um par de HA. Para adicionar pares de HA, seu sistema de arquivos deve ser configurado com pelo menos 1.536 MBps de capacidade de taxa de transferência.

First-generation Multi-AZ file system

Essas especificações de desempenho se aplicam aos sistemas de arquivos Multi-AZ de primeira geração criados após 28 de novembro de 2022 nas Regiões da AWS especificadas.

Especificações de desempenho para sistemas de arquivos nos seguintes Regiões da AWS: Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon) e Europa (Irlanda)

FSx capacidade de produção () MBps	Capacidade de taxa de transferência da rede () MBps		IOPS de rede	Armazenamento em cache na memória (GB)	NVMe armazenamento em cache (GB)	Taxa de transferência de disco () MBps		IOPS de unidade SSD *	
	Linha de base	Intermitência				Linha de base	Intermitência	Linha de base	Intermitência
128	188	1.500	Linha de base de dezenas de milhares	16	238	128	1.250	6.000	40.000
256	375	1.500		32	475	256	1.250	12.000	40.000
512	750	1.500		64	950	512	1.250	20.000	40.000
1,024	1.500	–		128	1.900	1,024	1.250	40.000	–
2.048	3.125	–		256	3.800	2.048	–	80.000	–
4.096	6.250	–		512	7.600	4.096	–	160.000	–

> **Note**
>
> * Seu SSD IOPS só é usado quando você acessa dados que não estão em cache no cache ou cache na memória do seu servidor de arquivos. NVMe

Essas especificações de desempenho se aplicam aos sistemas de arquivos Multi-AZ de primeira geração em todos os outros Regiões da AWS lugares FSx em que o ONTAP está disponível.

Especificações de desempenho para sistemas de arquivos em [todos os outros Regiões da AWS lugares onde FSx o ONTAP está disponível]

FSx capacidade de produção () MBps	Capacidade de taxa de transferência da rede () MBps		IOPS de rede	Armazenamento em cache na memória (GB)	NVMe armazenamento em cache (GB)	Taxa de transferência de disco () MBps		IOPS de unidade SSD *	
	Linha de base	Intermitência				Linha de base	Intermitência	Linha de base	Intermitência
128	150	1.250	Linha de base de dezenas de milhares	16	150	128	600	6.000	18.750
256	300	1.250		32	300	256	600	12.000	18.750
512	625	1.250	Linha de base de centenas de milhares	64	600	512	600	18.750	–
1,024	1.500	–		128	1.200	1,024	–	40.000	–
2.048	3.125	–		256	2.400	2.048	–	80.000	–

> **Note**
>
> * Seu SSD IOPS só é usado quando você acessa dados que não estão em cache no cache ou cache na memória do seu servidor de arquivos. NVMe

Second-generation Multi-AZ file systems

Essas especificações de desempenho se aplicam aos sistemas de arquivos Multi-AZ de segunda geração.

Especificações de desempenho dos sistemas de arquivos Multi-AZ de segunda geração

FSx capacidade de produção () MBps	Capacidade de taxa de transferência da rede () MBps		IOPS de rede	Armazenamento em cache na memória (GB)	NVMe armazenamento em cache (GB)	Taxa de transferência de disco () MBps		IOPS de unidade SSD *	
	Linha de base	Intermitência				Linha de base	Intermitência	Linha de base	Intermitência
384	781	6.250	Linha de base de centenas de milhares	16	237	384	3.125	12.500	65.000
768	1.563	6.250		32	474	768	3.125	25.000	65.000
1.536	3.125	6.250		64	950	1.536	3.125	50.000	65.000
3.072	6.250	–		128	1.900	3.072	–	100.000	–
6,144	12.500	–		256	3.800	6,144	–	200.000	–

> **Note**
>
> * Seu SSD IOPS só é usado quando você acessa dados que não estão em cache no cache ou cache na memória do seu servidor de arquivos. NVMe

Exemplo: capacidade de armazenamento e capacidade de throughput

O exemplo a seguir ilustra como a capacidade de armazenamento e a capacidade de throughput afetam a performance do sistema de arquivos.

Um sistema de arquivos de primeira geração configurado com 2 TiB de capacidade de armazenamento SSD e MBps 512 de capacidade de taxa de transferência tem os seguintes níveis de taxa de transferência:

- Taxa de transferência de rede — 625 de MBps linha de base e 1.250 de MBps intermitência (consulte a tabela de capacidade de taxa de transferência)
- Taxa de transferência de disco — 512 de linha de MBps base e 600 de intermitência. MBps

Portanto, sua carga de trabalho acessando o sistema de arquivos poderá gerar até 625 taxas de transferência de MBps linha de base e 1.250 de MBps intermitência para operações de arquivo executadas em dados acessados ativamente armazenados em cache no cache e no cache da memória do servidor de arquivos. NVMe

Administrando os recursos FSx do ONTAP

Usando a CLI e a API do AWS Management Console AWS CLI, e do ONTAP, você pode realizar as seguintes ações administrativas FSx para os recursos do ONTAP:

- Criação, listagem, atualização e exclusão de sistemas de arquivos, máquinas virtuais de armazenamento (SVMs), volumes, backups e tags.
- Gerenciar acesso, contas administrativas e senhas, requisitos de senha, protocolos SMB e iSCSI, acessibilidade de rede para os destinos de montagem dos sistemas de arquivos existentes

Tópicos

- Como gerenciar a capacidade de armazenamento
- Gerenciamento FSx para sistemas de arquivos ONTAP
- Gerenciamento FSx de máquinas virtuais de armazenamento ONTAP
- Gerenciamento FSx de volumes ONTAP
- Como criar um LUN de iSCSI
- Otimizando o desempenho com as janelas de FSx manutenção da Amazon
- Como gerenciar a capacidade de throughput
- Como gerenciar compartilhamentos de SMB
- Gerenciando FSx recursos do ONTAP usando NetApp aplicações
- Marcação de recursos da Amazon FSx

Como gerenciar a capacidade de armazenamento

O Amazon FSx for NetApp ONTAP fornece vários recursos relacionados ao armazenamento que você pode usar para gerenciar a capacidade de armazenamento em seu sistema de arquivos.

Tópicos

- FSx para níveis de armazenamento ONTAP
- Escolha da quantidade certa de armazenamento SSD do sistema de arquivos
- Capacidade de armazenamento e IOPS do sistema de arquivos
- Capacidade de armazenamento do volume

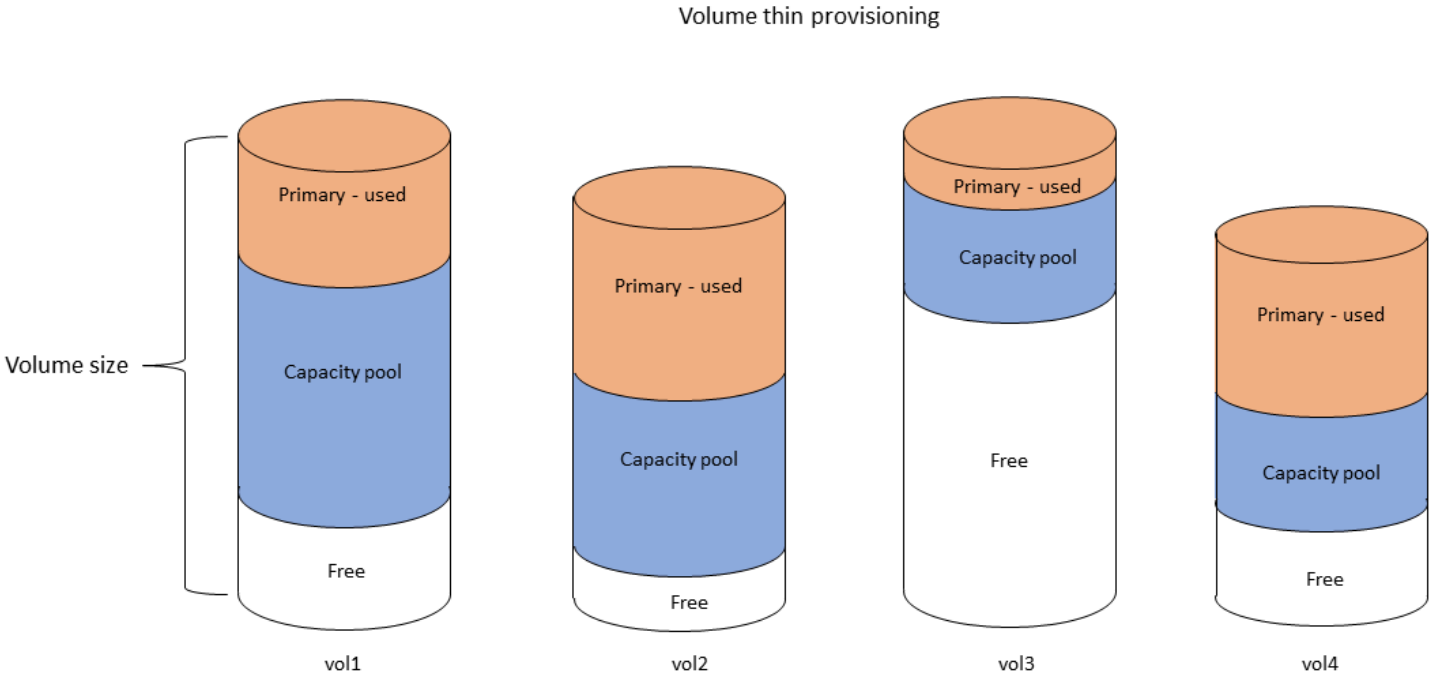
FSx para níveis de armazenamento ONTAP

As camadas de armazenamento são a mídia física de armazenamento de um sistema de arquivos Amazon FSx for NetApp ONTAP. FSx for ONTAP oferece os seguintes níveis de armazenamento:

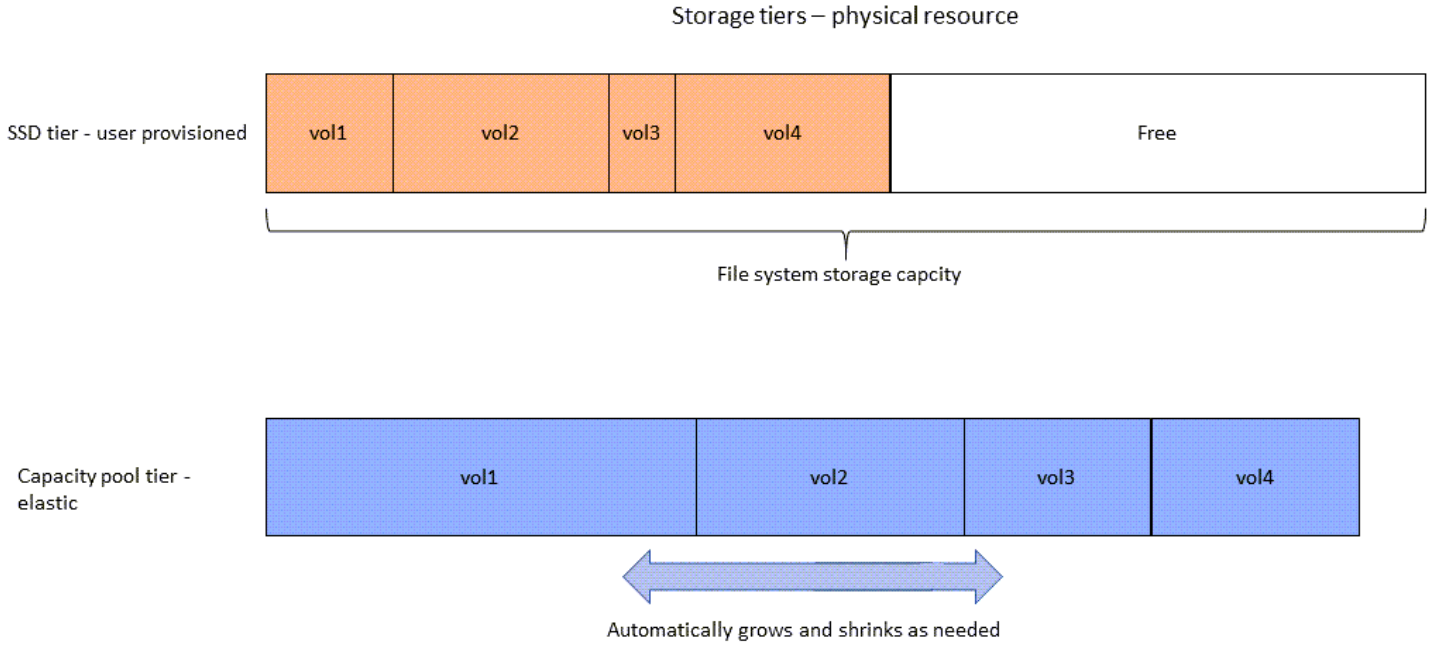
- Nível SSD: o armazenamento em unidade de estado sólido (SSD) de alta performance e provisionado pelo usuário, criado especificamente para a parte ativa do seu conjunto de dados.
- Nível do grupo de capacidade: armazenamento totalmente elástico cujo tamanho é escalado automaticamente para petabytes, sendo otimizado em termos de custo para os dados acessados com pouca frequência.

Um volume FSx for ONTAP é um recurso virtual que, semelhante às pastas, não consome capacidade de armazenamento. Os dados armazenados, que consomem armazenamento físico, residem em volumes. Ao criar um volume, você especifica seu tamanho, que pode ser modificado depois de criado. FSx para ONTAP, os volumes são provisionados de forma reduzida e o armazenamento do sistema de arquivos não é reservado com antecedência. Em vez disso, o armazenamento SSD e do grupo de capacidade são alocados dinamicamente, conforme necessário. Uma política de divisão em níveis, configurada no nível do volume, determina se e quando os dados armazenados no nível SSD fazem a transição para o nível do grupo de capacidade.

O diagrama a seguir ilustra um exemplo de dados dispostos em vários FSx volumes do ONTAP em um sistema de arquivos.



O diagrama a seguir ilustra como a capacidade de armazenamento físico do sistema de arquivos é consumida pelos dados nos quatro volumes do diagrama anterior.



Você pode reduzir seus custos de armazenamento escolhendo a política de divisão em níveis que melhor atenda aos requisitos de cada volume no sistema de arquivos. Para obter mais informações, consulte Divisão de dados em níveis no volume.

Escolha da quantidade certa de armazenamento SSD do sistema de arquivos

Ao escolher a quantidade de capacidade de armazenamento SSD FSx para seu sistema de arquivos ONTAP, você precisa ter em mente os seguintes itens que afetam a quantidade de armazenamento SSD disponível para armazenar seus dados:

- Capacidade de armazenamento reservada para a sobrecarga do software NetApp ONTAP.
- Metadados de arquivo
- Dados gravados recentemente
- Arquivos que você pretende armazenar no armazenamento SSD, sejam eles dados que não atingiram o período de resfriamento ou dados lidos recentemente e que foram recuperados no SSD.

Como o armazenamento SSD é usado

O armazenamento SSD do seu sistema de arquivos é usado para uma combinação do software NetApp ONTAP (sobrecarga), metadados de arquivos e seus dados.

NetApp Sobrecarga do software ONTAP

Como outros sistemas de arquivos NetApp ONTAP, até 16% da capacidade de armazenamento SSD de um sistema de arquivos é reservada para a sobrecarga do ONTAP, o que significa que ele não está disponível para armazenar seus arquivos. A sobrecarga do ONTAP é alocada da seguinte forma:

- 11% é reservado para o software NetApp ONTAP. Para sistemas de arquivos com mais de 30 tebibytes (TiB) de capacidade de armazenamento SSD, a reserva é de 6%.
- 5% são reservados para snapshots agregados, necessários na sincronização de dados entre os dois servidores de arquivos do sistema de arquivos.

Metadados de arquivo

Os metadados de arquivos normalmente consomem de 3 a 7% da capacidade de armazenamento consumida pelos arquivos. Essa porcentagem depende do tamanho médio do arquivo (um tamanho médio de arquivo menor requer mais metadados) e da quantidade de economia com a eficiência de armazenamento obtida nos arquivos. Observe que os metadados do arquivo não se beneficiam da economia com a eficiência de armazenamento. Você pode usar as diretrizes a seguir para estimar a quantidade de armazenamento SSD usada para os metadados no sistema de arquivos.

Tamanho médio do arquivo	Tamanho dos metadados como porcentagem dos dados do arquivo
4 KB	7%
8 KB	3,5%
32 KB ou maior	1-3%

Ao dimensionar a quantidade de capacidade de armazenamento SSD necessária para os metadados dos arquivos que planeja armazenar no nível do grupo de capacidade, recomendamos usar uma

proporção conservadora de 1 GiB de armazenamento SSD para cada 10 GiB de dados que planeja armazenar no nível do grupo de capacidade.

Dados de arquivos armazenados no nível SSD

Além do conjunto de dados ativo e de todos os metadados do arquivo, todos os dados gravados no sistema de arquivos são inicialmente gravados no nível SSD antes de serem divididos em níveis para o armazenamento do grupo de capacidade. Isso é verdade independentemente da política de hierarquização do volume, com a exceção de que os dados são gravados diretamente no armazenamento do pool de capacidade quando usados SnapMirror em um volume configurado com uma política de classificação de todos os dados.

As leituras aleatórias do nível do grupo de capacidade são armazenadas em cache no nível SSD, desde que ele esteja abaixo de 90% de utilização. Para obter mais informações, consulte Divisão de dados em níveis no volume.

Utilização recomendada da capacidade do SSD

Recomendamos que você não ultrapasse continuamente 80% de utilização do nível de armazenamento SSD. Para sistemas de arquivos de segunda geração, também recomendamos que você não ultrapasse continuamente 80% de utilização de nenhum dos agregados do seu sistema de arquivos. Essas recomendações são consistentes com NetApp a recomendação do ONTAP. Como o nível SSD do sistema de arquivos também é usado para preparar gravações e leituras aleatórias do nível do grupo de capacidade, qualquer mudança repentina nos padrões de acesso pode fazer com que a utilização do nível SSD aumente rapidamente.

Com 90% de utilização do SSD, os dados lidos do nível do grupo de capacidade não são mais armazenados em cache no nível SSD, de modo que a capacidade restante do SSD seja preservada para quaisquer novos dados gravados no sistema de arquivos. Isso faz com que as leituras repetidas dos mesmos dados do nível do grupo de capacidade sejam lidas no armazenamento do grupo de capacidade em vez de serem armazenadas em cache e lidas no nível SSD, o que pode afetar a capacidade de throughput do sistema de arquivos.

Toda a funcionalidade de divisão em níveis é interrompida quando o nível SSD atinge ou ultrapassa 98% de utilização. Para obter mais informações, consulte Limites de divisão em níveis.

Eficiência de armazenamento

NetApp ONTAP oferece recursos de eficiência de armazenamento em nível de bloco em nível de volume que incluem compactação, compactação e desduplicação. Esses recursos podem

economizar até 65% na capacidade de armazenamento para compartilhamentos gerais de arquivos, sem sacrificar o desempenho. Você pode habilitar a eficiência do armazenamento por volume. Esses recursos reduzem a quantidade de capacidade de armazenamento que seus dados consomem, permitindo que você consuma menos espaços de armazenamento em SSD, pool de capacidade e armazenamento de backups. Você pode habilitar a compactação e a desduplicação em cada volume para dados no armazenamento SSD. A economia de armazenamento decorrente da compactação e desduplicação no armazenamento SSD é preservada quando os dados são escalonados para o armazenamento do grupo de capacidade. A eficiência de armazenamento sempre estará habilitada para dados de backup, independentemente da configuração de eficiência de armazenamento do seu sistema de arquivos.

A tabela a seguir mostra exemplos habituais de economias de armazenamento.

	Somente compressão	Somente desduplicação	Compressão e desduplicação
Compartilhamentos de arquivos de uso geral	50%	30%	65%
Servidores e desktops virtuais	55%	70%	70%
Bancos de dados	65-70%	0%	65-70%
Dados de engenharia	55%	30%	75%
Dados geossísmicos	40%	3%	40%

Para a maioria das workloads, habilitar a compressão e a desduplicação não afetará negativamente o desempenho do sistema de arquivos. Para a maioria das workloads, a compactação aumenta o desempenho geral. Para fornecer leituras e gravações rápidas a partir do cache de RAM, FSx os servidores de arquivos do ONTAP são equipados com níveis mais altos de largura de banda de rede nas placas de interface de rede front-end (NICs) do que os disponíveis entre os servidores de arquivos e os discos de armazenamento. Como a compressão de dados reduz a quantidade de dados enviados entre servidores de arquivos e discos de armazenamento, na maioria das workloads, você visualizará um aumento na capacidade de throughput geral do sistema de arquivos ao usar a

compressão de dados. Os aumentos na capacidade de throughput relacionados à compressão de dados ficarão limitados quando você saturar a NIC do front-end do sistema de arquivos.

O Amazon FSx for NetApp ONTAP também suporta outros ONTAP recursos que economizam espaço, incluindo instantâneos, provisionamento reduzido e volumes. FlexClone

Os recursos de eficiência de armazenamento não estão habilitados por padrão. É possível habilitá-los dos modos a seguir.

- No volume raiz de uma SVM, ao criar um sistema de arquivos.
- Ao criar um volume.
- Ao modificar um volume existente.

Para ver a quantidade de economia de armazenamento em um sistema de arquivos com a eficiência de armazenamento habilitada, consulte Como monitorar a economia da eficiência de armazenamento.

Cálculo da economia com a eficiência do armazenamento

Você pode usar as métricas `LogicalDataStored` e `StorageUsed` FSx para o sistema de CloudWatch arquivos ONTAP para calcular a economia de armazenamento com compactação, desduplicação, compactação, instantâneos e FlexClones. Essas métricas têm uma única dimensão,`FileSystemId`. Para obter mais informações, consulte Métricas do sistema de arquivos.

- Para computar a economia com a eficiência de armazenamento em bytes, pegue a média de `StorageUsed` em um determinado período e subtraia da média de `LogicalDataStored` do mesmo período.
- Para computar a economia com a eficiência do armazenamento como uma porcentagem do tamanho lógico total dos dados, pegue a `Average` de `StorageUsed` em um determinado período e subtraia da `Average` de `LogicalDataStored` no mesmo período. Em seguida, divida a diferença pela `Average` de `LogicalDataStored` no mesmo período.

Exemplo de dimensionamento do SSD

Suponha que você queira armazenar 100 TiB de dados para uma aplicação em que 80% dos dados são acessados com pouca frequência. Nesse cenário, 80% (80 TiB) dos seus dados são automaticamente colocados em camadas no nível do pool de capacidade e os 20% restantes

(20 TiB) permanecem no armazenamento SSD. Com base na economia típica de 65% com a eficiência de armazenamento para workloads de compartilhamento de arquivos de uso geral, isso equivale a 7 TiB de dados. Para manter uma taxa de utilização de 80% do SSD, você precisa de 8,75 TiB de capacidade de armazenamento SSD para os 20 TiB de dados acessados ativamente. A quantidade provisionada de armazenamento SSD também precisa considerar a sobrecarga de 16% de armazenamento do software ONTAP, conforme mostrado no cálculo a seguir.

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

Portanto, neste exemplo, é necessário provisionar pelo menos 10,42 TiB de armazenamento SSD. Você também usará 28 TiB de armazenamento do grupo de capacidade para os 80 TiB restantes de dados acessados com pouca frequência.

Capacidade de armazenamento e IOPS do sistema de arquivos

Ao criar um sistema de arquivos FSx para ONTAP, você especifica a capacidade de armazenamento da camada SSD. Para sistemas de arquivos Single-AZ de segunda geração, a capacidade de armazenamento especificada é distribuída uniformemente entre os grupos de armazenamento de cada par de alta disponibilidade (HA); esses grupos de armazenamento são chamados de agregados.

Para cada GiB de armazenamento SSD que você provisiona, a Amazon provisiona FSx automaticamente 3 operações de entrada/saída de SSD por segundo (IOPS) para o sistema de arquivos, até um máximo de 160.000 SSD IOPS por sistema de arquivos. Para sistemas de arquivos Single-AZ de segunda geração, as IOPS de SSD são distribuídas uniformemente em cada um dos agregados do seu sistema de arquivos. Você tem a opção de especificar um nível de IOPS de SSD provisionado acima das três IOPS de SSD automáticos por GiB. Para obter mais informações sobre o número máximo de IOPS SSD que você pode provisionar para o seu FSx sistema de arquivos ONTAP, consulte. Impacto da capacidade de throughput na performance

Tópicos

- Atualização do armazenamento SSD e IOPS do sistema de arquivos
- Como criar um alarme de utilização da capacidade de armazenamento para seu sistema de arquivos
- Atualizar a capacidade de armazenamento e as IOPS provisionadas

- Atualizar a capacidade de armazenamento de maneira dinâmica
- Monitorar a utilização do armazenamento SSD
- Como monitorar a economia da eficiência de armazenamento
- Monitorar as atualizações da capacidade de armazenamento e das IOPS

Atualização do armazenamento SSD e IOPS do sistema de arquivos

Quando precisar de armazenamento adicional para a parte ativa do seu conjunto de dados, você pode aumentar a capacidade de armazenamento SSD do seu sistema de arquivos Amazon FSx for NetApp ONTAP. Use o FSx console da Amazon, a FSx API da Amazon ou AWS Command Line Interface (AWS CLI) para aumentar a capacidade de armazenamento SSD. Para obter mais informações, consulte Atualizar a capacidade de armazenamento e as IOPS provisionadas.

Quando você aumenta a capacidade de armazenamento SSD do seu sistema de FSx arquivos da Amazon, a nova capacidade normalmente fica disponível para uso em minutos. Será gerada uma cobrança pela nova capacidade de armazenamento SSD depois que ela estiver disponível para você. Para obter mais informações sobre preços, consulte Amazon FSx for NetApp ONTAP Pricing.

Depois de aumentar sua capacidade de armazenamento, a Amazon FSx executa um processo de otimização de armazenamento em segundo plano para reequilibrar seus dados. Na maioria dos sistemas de arquivos, a otimização do armazenamento leva algumas horas, com um impacto mínimo perceptível na performance da workload.

Você pode acompanhar o progresso do processo de otimização de armazenamento a qualquer momento usando o FSx console, a CLI e a API da Amazon. Para obter mais informações, consulte Monitorar as atualizações da capacidade de armazenamento e das IOPS.

Considerações

Veja a seguir alguns itens importantes a levar em consideração ao modificar a capacidade de armazenamento SSD e as IOPS provisionadas de um sistema de arquivos.

- Somente o aumento da capacidade de armazenamento: só é possível aumentar a quantidade da capacidade de armazenamento SSD de um sistema de arquivos; não é possível diminuir a capacidade de armazenamento.
- Aumento mínimo da capacidade de armazenamento: cada aumento na capacidade de armazenamento SSD deve ser no mínimo de 10% da capacidade atual de armazenamento

SSD do sistema de arquivos, até a capacidade máxima de armazenamento em SSD para a configuração do seu sistema de arquivos.

- (Somente sistemas de arquivos Single-AZ de segunda geração) Distribuição da capacidade de armazenamento: a nova capacidade de armazenamento ou de IOPS de SSD que você selecionar para seu sistema de arquivos será distribuída uniformemente em cada um dos agregados do seu sistema de arquivos.
- Tempo entre aumentos: após modificar a capacidade de armazenamento SSD, as IOPS provisionadas ou a capacidade de throughput em um sistema de arquivos, aguarde pelo menos seis horas antes de modificar qualquer uma dessas configurações no mesmo sistema de arquivos novamente. Às vezes isso é referenciado como período de desaquecimento.
- Modos de IOPS provisionadas: para uma alteração das IOPS provisionadas, especifique um dos dois modos de IOPS a seguir.
  - Modo automático — A Amazon escala FSx automaticamente suas IOPS de SSD para manter 3 IOPS de SSD provisionadas por GiB de capacidade de armazenamento de SSD, até o máximo de IOPS de SSD para sua configuração de sistema de arquivos.

    > **Note**
    >
    > Para obter mais informações sobre o número máximo de IOPS SSD que você pode provisionar para o seu FSx sistema de arquivos ONTAP, consulte. Impacto da capacidade de throughput na performance
  - Modo provisionado pelo usuário: você especifica o número de IOPS de SSD, que deve ser maior ou igual a três IOPS por GiB de capacidade de armazenamento SSD. Se você optar por provisionar um nível mais alto de IOPS, pagará pela média de IOPS provisionadas acima da taxa incluída no mês, medida em meses de IOPS.

Para obter mais informações sobre preços, consulte Amazon FSx for NetApp ONTAP Pricing.

Quando aumentar a capacidade de armazenamento de SSD

Se você estiver ficando sem armazenamento de nível SSD disponível, recomendamos aumentar a capacidade de armazenamento do sistema de arquivos. A falta de armazenamento indica que seu nível SSD está subdimensionado para a parte ativa do seu conjunto de dados.

Para monitorar a quantidade de armazenamento gratuito disponível no sistema de arquivos, use o nível do sistema de arquivos e as métricas `StorageCapacity` da `StorageUsed` Amazon

CloudWatch . Você pode criar um CloudWatch alarme em uma métrica e ser notificado quando ela cair abaixo de um limite específico. Para obter mais informações, consulte Monitoramento com a Amazon CloudWatch.

> **Note**
>
> Recomendamos que você não exceda 80% de utilização da capacidade de armazenamento SSD, para garantir que a divisão de dados em níveis, a escalabilidade do throughput e outras atividades de manutenção funcionem adequadamente, além de que haja capacidade disponível para dados adicionais. Para sistemas de arquivos de segunda geração, essa recomendação se aplica tanto à utilização média de todos os agregados do sistema de arquivos quanto a cada agregado individual.

Para obter mais informações sobre como o armazenamento SSD de um sistema de arquivos é usado e a quantidade de armazenamento SSD reservada para metadados de arquivos e software operacional, consulte Escolha da quantidade certa de armazenamento SSD do sistema de arquivos.

Como criar um alarme de utilização da capacidade de armazenamento para seu sistema de arquivos

Recomendamos que você não exceda continuamente uma utilização média de 80% da capacidade de armazenamento SSD. Picos ocasionais de utilização do armazenamento SSD acima de 80% são aceitáveis. Manter uma utilização média abaixo de 80% fornece capacidade suficiente para aumentar seu armazenamento sem encontrar problemas. O procedimento a seguir mostra como criar um CloudWatch alarme que alerta quando a utilização do armazenamento SSD do seu sistema de arquivos está se aproximando de 80%.

Criar um alarme de utilização da capacidade de armazenamento do sistema de arquivos

Você pode usar a `StorageCapacityUtilization` métrica para criar um alarme que é acionado quando um ou mais dos seus sistemas de arquivos FSx for ONTAP atingem um limite de utilização de armazenamento.

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação esquerdo, em Alarmes, escolha Todos os alarmes. Em seguida, escolha Criar alarme. No assistente de criação de alarme, escolha Selecionar métrica.
3. No explorador de gráficos, escolha a guia Consulta a várias fontes.

4. No criador de consultas, escolha o seguinte:
   - Para Namespace, selecione AWS/FSx> Métricas detalhadas do sistema de arquivos.
   - Em Nome da métrica, selecione MAX (StorageCapacityUtilization).
   - Em Filtrar por, você terá a opção de incluir ou excluir sistemas de arquivos específicos por ID. Se você deixar o campo Filtrar por vazio, seu alarme será acionado quando qualquer um dos seus sistemas de arquivos exceder o limite de utilização da capacidade de armazenamento do alarme.
   - Deixe os valores das opções restantes em branco e escolha Representar consulta graficamente.
5. Escolha Selecionar métrica. De volta ao assistente, na seção Métrica, atribua um rótulo à sua métrica. Recomendamos manter o Período em 5 minutos.
6. Em Condições, escolha o Tipo de limite estático sempre que sua métrica for Maior/igual a 80.
7. Escolha Avançar para acessar a página Configurar ações.

Para configurar ações de alarme

Você pode configurar diversas ações para que seu alarme seja acionado quando atingir o limite que você configurou. Neste exemplo, escolhemos um tópico do Simple Notification Service (SNS), mas você pode aprender sobre outras ações em Usando CloudWatch alarmes da Amazon no Guia do usuário da Amazon. CloudWatch

1. N seção Notificação, escolha um tópico do SNS para notificar quando o alarme estiver no estado `ALARM`. Você pode escolher um tópico existente ou criar um novo tópico. Você receberá uma notificação de assinatura que precisa confirmar antes de receber notificações de alarme no endereço de e-mail.
2. Escolha Próximo.

Para finalizar o alarme

Siga estas instruções para concluir o processo de criação do CloudWatch alarme.

1. Na página Adicionar nome e descrição, dê um nome ao alarme e, opcionalmente, uma descrição e escolha Avançar.
2. Revise tudo o que você configurou na página Visualizar e criar e, em seguida, escolha Criar alarme.

Atualizar a capacidade de armazenamento e as IOPS provisionadas

Você pode aumentar o armazenamento baseado em SSD de um sistema de arquivos e aumentar ou diminuir a quantidade de IOPS SSD provisionadas usando o console da FSx Amazon, AWS CLI o e a API.

Atualizar a capacidade de armazenamento SSD ou as IOPS provisionadas de um sistema de arquivos (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, selecione Sistemas de arquivos. Na lista Sistemas de arquivos, selecione o sistema de arquivos ONTAP FSx para o qual você deseja atualizar a capacidade de armazenamento SSD e o IOPS do SSD.
3. Escolha Ações > Atualizar capacidade de armazenamento. Como alternativa, na seção Resumo, escolha Atualizar ao lado do valor da Capacidade de armazenamento SSD do sistema de arquivos.

   A caixa de diálogo Atualizar capacidade de armazenamento SSD e IOPS é exibida.

Update SSD storage capacity and IOPS

File system ID

fs-01234567890abcdef

Current configuration

SSD storage capacity: 4096 GiB
IOPS mode: Automatic (3 IOPS per GiB of SSD storage)
SSD IOPS: 12288

SSD storage capacity

☑ Modify storage capacity

Input type

◉ Percentage
○ Absolute

Desired % increase

10 %

Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.

Provisioned SSD IOPS

◉ Automatic (3 IOPS per GiB of SSD storage)
○ User-provisioned

Configuration preview

Attribute	Current configuration	New configuration
SSD storage capacity	4,096 GiB (2,048 GiB per HA pair)	4,506 GiB (2,253 GiB per HA pair)
	Mode: Automatic	Mode: Automatic

4. Para aumentar a capacidade de armazenamento SSD, escolha Modificar capacidade de armazenamento.
5. Em Tipo de entrada, selecione uma das opções a seguir.
   - Para inserir a nova capacidade de armazenamento SSD como uma alteração percentual em relação ao valor atual, escolha Porcentagem.
   - Para inserir o novo valor em GiB, escolha Absoluto.
6. Dependendo do tipo de entrada, insira um valor em % de aumento desejado.
   - Em Porcentagem, insira o valor do aumento percentual. Esse valor deve ser pelo menos 10% maior que o valor atual.
   - Em Absoluto, insira o novo valor em GiB, até o valor máximo permitido de 196.608 GiB.
7. Em IOPS provisionadas de SSD, você tem as duas opções a seguir para modificar o número de IOPS provisionadas de SSD do sistema de arquivos.
   - Se você quiser que FSx a Amazon escale automaticamente suas IOPS de SSD para manter 3 IOPS de SSD provisionadas por GiB de capacidade de armazenamento SSD (até um máximo de 160.000), escolha Automático.
   - Se quiser especificar o número de IOPS de SSD, escolha Provisionado pelo usuário. Insira um número absoluto de IOPS que seja, pelo menos, três vezes a quantidade de GiB do nível de armazenamento SSD e menor ou igual a 160.000.

   > **Note**
   >
   > Para obter mais informações sobre o número máximo de IOPS SSD que você pode provisionar para o seu FSx sistema de arquivos ONTAP, consulte. Impacto da capacidade de throughput na performance
8. Selecione Atualizar.

   > **Note**
   >
   > Na parte inferior do prompt, o sistema exibirá uma prévia da configuração com sua nova capacidade de armazenamento SSD e IOPS de SSD. Para sistemas de arquivos de segunda geração, o per-HA-pair valor também é mostrado.

Atualizar a capacidade de armazenamento SSD e as IOPS provisionadas de um sistema de arquivos (CLI)

Para atualizar a capacidade de armazenamento SSD e as IOPS provisionadas de um sistema de arquivos FSx for ONTAP, use o AWS CLI comando update-file-systemou a ação de API equivalente. UpdateFileSystem Defina os parâmetros a seguir com seus valores:

- Defina `--file-system-id` como o ID do sistema de arquivos que está sendo atualizado.
- Para aumentar a capacidade de armazenamento SSD, defina `--storage-capacity` como um valor de capacidade de armazenamento de destino, que deverá ser no mínimo 10% maior que o valor atual.
- Para modificar as IOPS provisionadas de SSD, use a propriedade `--ontap-configuration DiskIopsConfiguration`. Essa propriedade tem dois parâmetros, `Iops` e `Mode`:
  - Se quiser especificar o número de IOPS provisionadas, use `Iops=`*`number_of_IOPS`* (até um máximo de 160.000) e `Mode=USER_PROVISIONED`. O valor de IOPS deve ser maior ou igual a três vezes a capacidade de armazenamento SSD solicitada. Se você não estiver aumentando a capacidade de armazenamento, o IOPs valor deverá ser maior ou igual a três vezes a capacidade de armazenamento SSD atual.
  - Se você quiser que FSx a Amazon aumente automaticamente seu SSD IOPS, use `Mode=AUTOMATIC` e não use o `Iops` parâmetro. A Amazon FSx manterá automaticamente 3 SSD IOPS por GiB da capacidade de armazenamento SSD provisionada (até um máximo de 160.000).

> **Note**
>
> Para obter mais informações sobre o número máximo de IOPS SSD que você pode provisionar para o seu FSx sistema de arquivos ONTAP, consulte. Impacto da capacidade de throughput na performance

O exemplo a seguir aumenta o armazenamento SSD do sistema de arquivos para 2.000 GiB e define para 7.000 a quantidade de IOPS de SSD provisionadas ao usuário.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 2000 \
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

Para monitorar o progresso da atualização, use o describe-file-systems AWS CLI comando. Procure a seção `AdministrativeActions` na saída.

Para obter mais informações, consulte AdministrativeActiona Referência da API Amazon FSx for NetApp ONTAP.

Atualizar a capacidade de armazenamento de maneira dinâmica

Você pode usar a solução a seguir para aumentar dinamicamente a capacidade de armazenamento SSD de um sistema de arquivos FSx for ONTAP quando a quantidade de capacidade de armazenamento SSD usada exceder um limite especificado por você. Esse AWS CloudFormation modelo implanta automaticamente todos os componentes necessários para definir o limite de capacidade de armazenamento, o CloudWatch alarme da Amazon com base nesse limite e a AWS Lambda função que aumenta a capacidade de armazenamento do sistema de arquivos.

A solução implanta automaticamente todos os componentes necessários e usa os parâmetros a seguir.

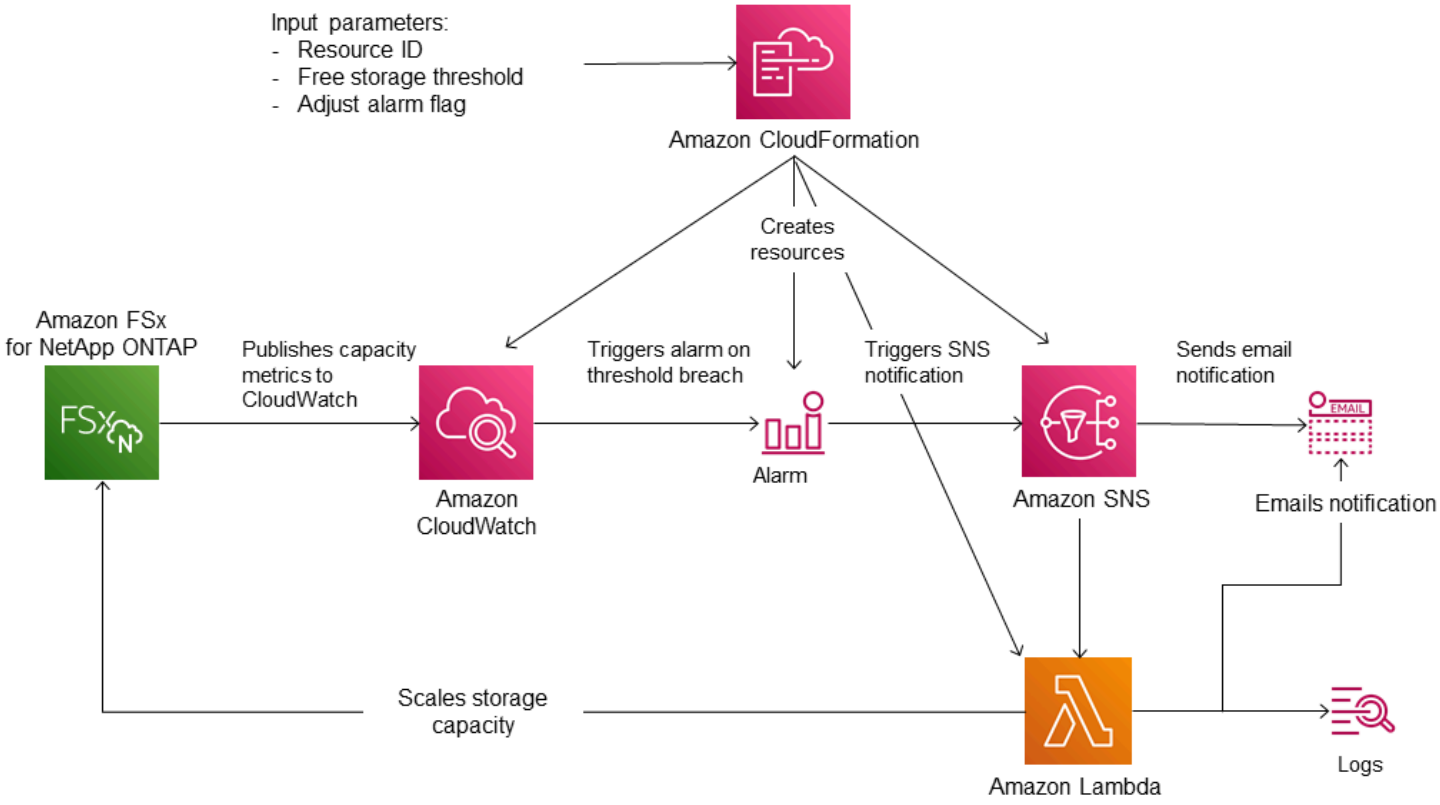
- Seu ID FSx do sistema de arquivos ONTAP.
- O limite da capacidade de armazenamento SSD usada (valor numérico). Essa é a porcentagem na qual o CloudWatch alarme será acionado.
- A porcentagem pela qual aumentar a capacidade de armazenamento (%).
- O endereço de e-mail usado para receber notificações de escalabilidade.

Tópicos

- Visão geral da arquitetura
- AWS CloudFormation modelo
- Implantação automatizada com AWS CloudFormation

Visão geral da arquitetura

A implantação dessa solução cria os recursos apresentados a seguir na Nuvem AWS.



O diagrama ilustra as seguintes etapas:

1. O AWS CloudFormation modelo implanta um CloudWatch alarme, uma AWS Lambda função, uma fila do Amazon Simple Notification Service (Amazon SNS) e todas as funções necessárias (IAM). AWS Identity and Access Management A função do IAM dá permissão à função Lambda para invocar as operações de API da Amazon FSx .
2. CloudWatch aciona um alarme quando a capacidade de armazenamento usada pelo sistema de arquivos excede o limite especificado e envia uma mensagem para a fila do Amazon SNS. Um alarme é acionado somente quando a capacidade usada pelo sistema de arquivos excede continuamente o limite por um período de cinco minutos.
3. Em seguida, a solução aciona a função do Lambda que está inscrita nesse tópico do Amazon SNS.
4. A função do Lambda calcula a nova capacidade de armazenamento do sistema de arquivos com base no valor percentual de aumento especificado e define a nova capacidade de armazenamento do sistema de arquivos.
5. O estado original do CloudWatch alarme e os resultados das operações da função Lambda são enviados para a fila do Amazon SNS.

Para receber notificações sobre as ações que são executadas como resposta ao CloudWatch alarme, você deve confirmar a assinatura do tópico do Amazon SNS seguindo o link fornecido no e-mail de confirmação da assinatura.

AWS CloudFormation modelo

Essa solução é usada AWS CloudFormation para automatizar a implantação dos componentes usados para aumentar automaticamente a capacidade de armazenamento de um sistema de arquivos FSx for ONTAP. Para usar essa solução, baixe o FSxOntapDynamicStorageScaling AWS CloudFormation modelo.

O modelo usa os Parâmetros descritos a seguir. Revise os parâmetros do modelo e seus valores padrão, modificando-os de acordo com as necessidades do seu sistema de arquivos.

FileSystemId

Nenhum valor padrão. O ID do sistema de arquivos para o qual você deseja aumentar automaticamente a capacidade de armazenamento.

LowFreeDataStorageCapacityThreshold

Nenhum valor padrão. Especifica o limite da capacidade de armazenamento usado, no qual acionar um alarme e aumentar automaticamente a capacidade de armazenamento do sistema de arquivos, definido como porcentagem (%) da capacidade de armazenamento atual do sistema de arquivos. Considera-se que o sistema de arquivos tem baixa capacidade de armazenamento livre quando o armazenamento usado excede esse limite.

EmailAddress

Nenhum valor padrão. Especifica o endereço de e-mail a ser usado para a assinatura do SNS e recebe os alertas de limite da capacidade de armazenamento.

PercentIncrease

O padrão é 20%. Especifica a quantidade pela qual aumentar a capacidade de armazenamento, expressa como uma porcentagem da capacidade de armazenamento atual.

> **Note**
>
> O escalonamento do armazenamento é tentado uma vez toda vez que o CloudWatch alarme entra no `ALARM` estado. Se a utilização da capacidade de armazenamento

SSD permanecer acima do limite após uma tentativa de operação de escalabilidade de armazenamento, não será feita uma nova tentativa dessa operação.

Máximo FSx SizeinGi B

O padrão é 196608. Especifica a capacidade máxima de armazenamento compatível com o armazenamento SSD.

Implantação automatizada com AWS CloudFormation

O procedimento a seguir configura e implanta uma AWS CloudFormation pilha para aumentar automaticamente a capacidade de armazenamento de um sistema de arquivos FSx for ONTAP. A implantação leva alguns minutos. Para obter mais informações sobre a criação de uma CloudFormation pilha, consulte Como criar uma pilha no AWS CloudFormation console no Guia do AWS CloudFormation usuário.

> **Note**
>
> A implementação dessa solução gera cobrança pelos serviços associados AWS . Para obter mais informações, consulte as páginas de detalhes de preços desses serviços.

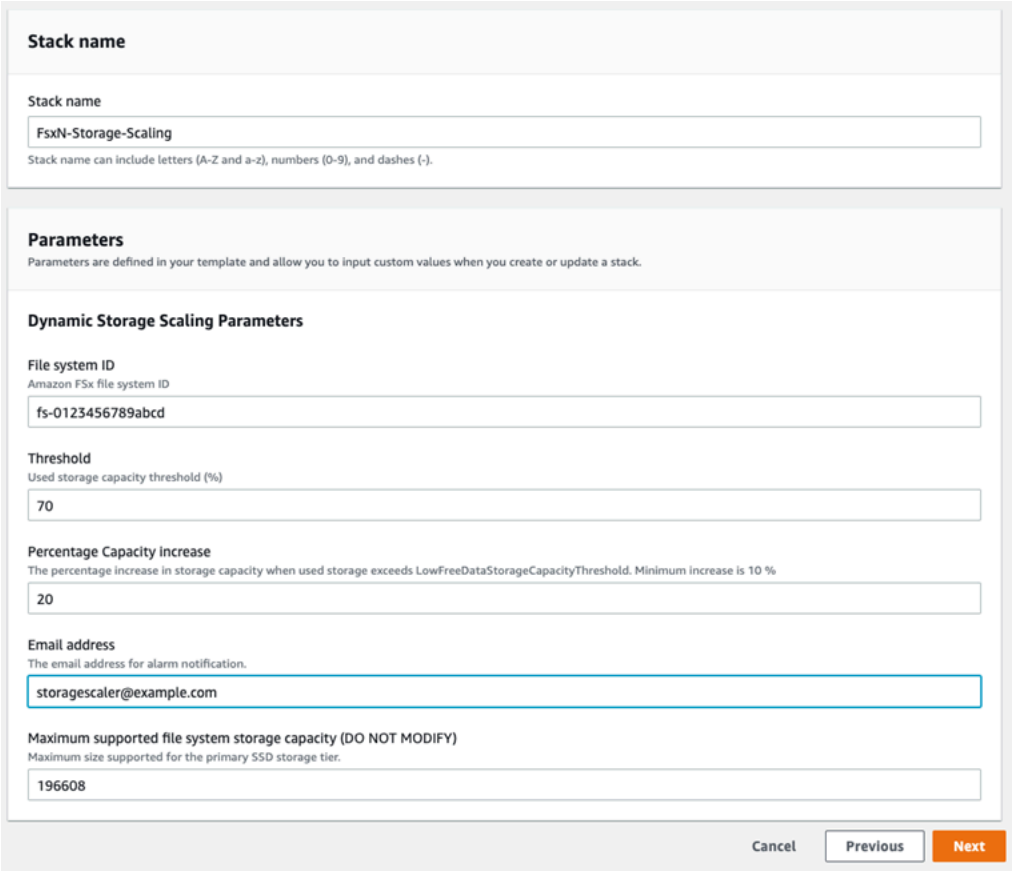
Antes de começar, você deve ter o ID do sistema de FSx arquivos da Amazon que está sendo executado na Amazon Virtual Private Cloud (Amazon VPC) em seu. Conta da AWS Para obter mais informações sobre a criação de FSx recursos da Amazon, consulteComeçando a usar a Amazon FSx para NetApp ONTAP.

Iniciar a pilha de soluções para o aumento automático da capacidade de armazenamento

1. Faça download do modelo do FSxOntapDynamicStorageScaling AWS CloudFormation .

   > **Note**
   >
   > No momento, a Amazon FSx está disponível apenas em AWS regiões específicas. Você deve iniciar essa solução em uma AWS região onde a Amazon FSx esteja disponível. Para obter mais informações, consulte FSx endpoints e cotas da Amazon no. Referência geral da AWS

2. No AWS CloudFormation console, escolha Criar pilha > Com novos recursos.
3. Selecione O modelo está pronto. Na seção Especificar modelo, escolha Fazer upload de um arquivo de modelo e faça o upload do modelo baixado.
4. Em Especificar detalhes da pilha, insira os valores da solução para o aumento automático da capacidade de armazenamento.



5. Insira um Nome da pilha.
6. Em Parâmetros, revise os parâmetros do modelo e modifique-os para atender às necessidades do seu sistema de arquivos. Escolha Próximo.

> **Note**
>
> Para receber notificações por e-mail quando esse CloudFormation modelo tentar escalar, confirme o e-mail de assinatura do SNS que você recebe após a implantação do modelo.

7. Insira as configurações de Opções que você deseja para a solução personalizada e escolha Próximo.

8. Em Analisar, revise e confirme as configurações da solução. Você deve selecionar a caixa de seleção confirmando que o modelo cria recursos do IAM.
9. Selecione Criar para implantar a stack.

Você pode ver o status da pilha no AWS CloudFormation console na coluna Status. Você verá um status de CREATE_COMPLETE em alguns minutos.

Atualizar a pilha

Depois que a pilha for criada, você poderá atualizá-la usando o mesmo modelo e fornecendo novos valores para os parâmetros. Para obter mais informações, consulte Atualizar pilhas diretamente no Guia do usuário do AWS CloudFormation .

Monitorar a utilização do armazenamento SSD

Você pode monitorar a utilização da capacidade de armazenamento SSD do seu sistema de arquivos usando uma variedade de e AWS NetApp ferramentas. Usando a Amazon, CloudWatch você pode monitorar a utilização da capacidade de armazenamento e definir alarmes para alertá-lo quando a utilização da capacidade de armazenamento atingir um limite personalizável.

> **Note**
>
> Recomendamos que você não exceda 80% da utilização da capacidade de armazenamento do seu nível de armazenamento SSD. Isso garante que a divisão em níveis funcione adequadamente e fornece sobrecarga para novos dados. Se nível de armazenamento SSD estiver consistentemente acima de 80% de utilização da capacidade de armazenamento, você poderá aumentar a capacidade do nível de armazenamento SSD. Para obter mais informações, consulte Atualização do armazenamento SSD e IOPS do sistema de arquivos.

Você pode ver o armazenamento SSD disponível em um sistema de arquivos e a distribuição geral do armazenamento no FSx console da Amazon. O gráfico Capacidade de armazenamento principal disponível exibe a quantidade de capacidade de armazenamento baseada em SSD disponível em um sistema de arquivos ao longo do tempo. O gráfico Distribuição de armazenamento mostra como a capacidade geral de armazenamento de um sistema de arquivos está atualmente distribuída em três categorias:

- Nível do grupo de capacidade

- Nível SSD disponível
- Nível SSD usado

Você pode monitorar a utilização da capacidade de armazenamento SSD do seu sistema de arquivos no AWS Management Console, usando o procedimento a seguir.

Monitorar a capacidade de armazenamento no nível SSD disponível no sistema de arquivos (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Escolha Sistemas de arquivos na coluna de navegação à esquerda e, em seguida, escolha a ONTAP sistema de arquivos do qual você deseja visualizar as informações de capacidade de armazenamento. A página de detalhes do sistema de arquivos é exibida.
3. No segundo painel, escolha a guia Monitoramento e desempenho e, em seguida, escolha Armazenamento. Os gráficos Capacidade de armazenamento principal disponível e Utilização da capacidade de armazenamento por agregado serão exibidos.

Como monitorar a economia da eficiência de armazenamento

Quando ativado, você pode ver quanta capacidade de armazenamento está economizando no console da Amazon, no FSx console da Amazon CloudWatch e na CLI do ONTAP.

Visualizar a economia da eficiência de armazenamento (console)

A economia de eficiência de armazenamento exibida no FSx console da Amazon FSx para um sistema de arquivos para ONTAP inclui a economia de FlexClones e. SnapShots

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Escolha o sistema de arquivos ONTAP FSx para o qual você deseja visualizar a economia de eficiência de armazenamento na lista de sistemas de arquivos.
3. Escolha Resumo na guia Monitoramento e desempenho no segundo painel na página de detalhes do sistema de arquivos.
4. O gráfico Economia com a eficiência de armazenamento mostra quanto espaço está sendo economizado como uma porcentagem do tamanho lógico dos dados e em bytes físicos.

Para ver a economia de eficiência de armazenamento (ONTAP CLI)

Você pode ver a economia de eficiência de armazenamento resultante apenas da compactação, compactação e desduplicação — sem os efeitos de instantâneos e FlexClones — executando o `storage aggregate show-efficiency` comando usando o ONTAP CLI. Para obter mais informações, consulte Storage Aggregate show-efficiency no NetApp ONTAP Centro de documentação.

1. Para acessar o ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.
2. O comando storage aggregate show-efficiency exibe informações sobre a eficiência de armazenamento de todos os agregados. A eficiência de armazenamento é exibida em quatro níveis diferentes:

   - Total
   - Agregar
   - Volume
   - Instantâneo e volume FlexClone

   ```
   ::*> aggr show-efficiency

   Aggregate: aggr1
        Node: node1

   Total Data Reduction Efficiency Ratio:  3.29:1
   Total Storage Efficiency Ratio:         4.29:1
   Aggregate: aggr2
        Node: node1

   Total Data Reduction Efficiency Ratio:  4.50:1
   Total Storage Efficiency Ratio:         5.49:1
   ```

```
cluster::*> aggr show-efficiency -details

Aggregate: aggr1
     Node: node1

Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1

Aggregate: aggr2
     Node: node1
Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

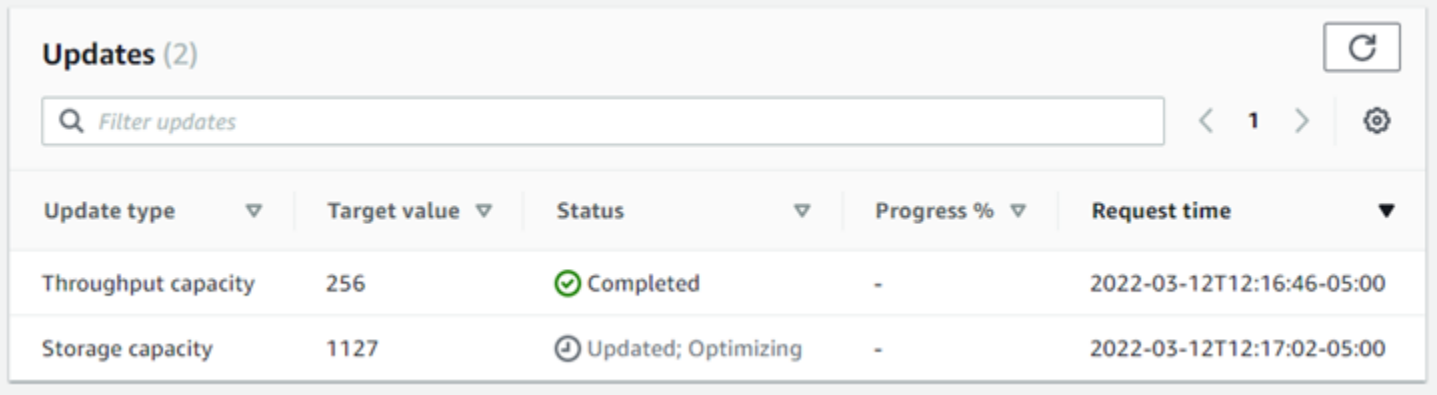
Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1
```

Monitorar as atualizações da capacidade de armazenamento e das IOPS

Você pode monitorar o progresso da capacidade de armazenamento SSD e da atualização de IOPS usando o FSx console, a CLI e a API da Amazon.

Para monitorar o armazenamento e as atualizações de IOPS (console)

Na guia Atualizações na página de detalhes do sistema de arquivos do seu sistema de arquivos FSx para ONTAP, você pode ver as 10 atualizações mais recentes para cada tipo de atualização.



Para atualizações da capacidade de armazenamento SSD e das IOPS, você pode ver as informações a seguir.

Tipo de atualização

Os tipos compatíveis são Capacidade de armazenamento, Modo e IOPS. Os valores de Modo e IOPS são listados para todas as solicitações de capacidade de armazenamento e escalabilidade de IOPS.

Target value (Valor de destino)

O valor especificado para atualizar a capacidade de armazenamento SSD ou as IOPS do sistema de arquivos.

Status

O status atual da atualização. Os valores possíveis são:

- Pendente — a Amazon FSx recebeu a solicitação de atualização, mas ainda não começou a processá-la.
- Em andamento — a Amazon FSx está processando a solicitação de atualização.
- Atualizado; Otimizando — a Amazon FSx aumentou a capacidade de armazenamento SSD do sistema de arquivos. Agora, o processo de otimização do armazenamento está reequilibrando seus dados em segundo plano.
- Concluída: a atualização foi concluída com êxito.
- Falha: a solicitação de atualização falhou. Escolha o ponto de interrogação (?) para ver os detalhes.

% de progresso

Exibe o progresso do processo de otimização do armazenamento como a porcentagem concluída.

Horário da solicitação

A hora em que a Amazon FSx recebeu a solicitação de ação de atualização.

Para monitorar o armazenamento e as atualizações de IOPS (CLI)

Você pode visualizar e monitorar as solicitações de aumento da capacidade de armazenamento SSD do sistema de arquivos usando o describe-file-systems AWS CLI comando e a operação da DescribeFileSystemsAPI. A matriz `AdministrativeActions` lista as dez ações de atualização mais recentes para cada tipo de ação administrativa. Ao aumentar a capacidade de armazenamento SSD de um sistema de arquivos, duas ações `AdministrativeActions` são geradas: uma ação `FILE_SYSTEM_UPDATE` e uma `STORAGE_OPTIMIZATION`.

O exemplo apresentado a seguir mostra um trecho da resposta de um comando `describe-file-systems` da CLI. O sistema de arquivos tem uma ação administrativa pendente para aumentar a capacidade de armazenamento SSD para 2.000 GiB e as IOPS provisionadas de SSD para 7.000 GiB.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
             }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1586797629.095,
        "Status": "PENDING"
    }
]
```

A Amazon FSx processa a `FILE_SYSTEM_UPDATE` ação primeiro, adicionando os novos discos de armazenamento maiores ao sistema de arquivos. Quando o novo armazenamento estiver disponível para o sistema de arquivos, o status `FILE_SYSTEM_UPDATE` será alterado para `UPDATED_OPTIMIZING`. A capacidade de armazenamento mostra o novo valor maior e FSx a Amazon começa a processar a ação `STORAGE_OPTIMIZATION` administrativa. Esse comportamento é mostrado a seguir, no trecho da resposta de um comando de CLI `describe-file-systems`.

A propriedade `ProgressPercent` exibe o progresso do processo de otimização do armazenamento. Após o processo de otimização do armazenamento ser concluído com êxito, o status da ação `FILE_SYSTEM_UPDATE` mudará para `COMPLETED`, e a ação `STORAGE_OPTIMIZATION` não aparecerá mais.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586799169.445,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "ProgressPercent": 41,
        "RequestTime": 1586799169.445,
        "Status": "IN_PROGRESS"
    }
]
```

Se a solicitação de atualização da capacidade de armazenamento ou das IOPS falhar, o status da ação `FILE_SYSTEM_UPDATE` mudará para `FAILED`, conforme mostrado no exemplo a seguir. a propriedade `FailureDetails` fornece informações sobre a falha.

```
"AdministrativeActions": [
    {
```

```
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586373915.697,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

Capacidade de armazenamento do volume

FSx para ONTAP, os volumes são recursos virtuais que você usa para agrupar dados, determinar como os dados são armazenados e determinar o tipo de acesso aos seus dados. Os volumes, assim como as pastas, não consomem a capacidade de armazenamento do sistema de arquivos sozinhos. Somente os dados armazenados em um volume consomem o armazenamento SSD e, dependendo da política de divisão em níveis do volume, o armazenamento do grupo de capacidade. Você define o tamanho de um volume ao criá-lo e pode alterá-lo posteriormente. Você pode monitorar e gerenciar a capacidade de armazenamento de seus volumes FSx for ONTAP usando a AWS Management Console API AWS CLI e a CLI do ONTAP.

Tópicos

- Divisão de dados em níveis no volume
- Snapshots e capacidade de armazenamento de volumes
- Capacidade do arquivo de volumes
- Como gerenciar eficiências de armazenamento
- Habilitar o dimensionamento automático
- Habilitar o modo de gravação na nuvem
- Como atualizar a capacidade de armazenamento
- Atualizar uma política de camadas

- Atualizar o mínimo de dias de resfriamento
- Atualizar a política de recuperação na nuvem de um volume
- Atualizar o número máximo de arquivos em um volume
- Monitorar a capacidade de armazenamento de volumes
- Monitorar a capacidade de arquivos de um volume

Divisão de dados em níveis no volume

Um sistema de arquivos Amazon FSx for NetApp ONTAP tem dois níveis de armazenamento: armazenamento primário e armazenamento em pool de capacidade. O armazenamento principal é um armazenamento SSD provisionado, escalável e de alta performance, criado especificamente para a parte ativa do seu conjunto de dados. O armazenamento do grupo de capacidade é um nível de armazenamento totalmente elástico cujo tamanho pode ser escalado para petabytes, sendo otimizado em termos de custo para dados acessados com pouca frequência.

Os dados em cada volume são hierarquizados automaticamente em camadas no nível de armazenamento do grupo de capacidade com base na política de camadas, no período de resfriamento e nas configurações de limite do volume. As seções a seguir descrevem as políticas de camadas de volume do ONTAP e os limites usados para determinar quando os dados são hierarquizados no grupo de capacidade.

> **Note**
>
> FSx for ONTAP suporta a classificação de dados em camadas para o pool de capacidade em todos os SnapLock volumes, independentemente do SnapLock tipo. Para obter mais informações, consulte Como SnapLock funciona.

Políticas de camadas de volume

Você determina como usar seus níveis FSx de armazenamento do sistema de arquivos ONTAP escolhendo a política de classificação por níveis para cada volume no sistema de arquivos. Você escolhe a política de classificação por níveis ao criar um volume e pode modificá-la a qualquer momento com o FSx console da Amazon AWS CLI, a API ou usando ferramentas NetApp de gerenciamento. Você pode escolher uma das políticas a seguir que determinam quais dados, se houver algum, estão divididos em níveis no armazenamento do grupo de capacidade.

> **Note**
>
> A divisão em níveis pode mover seus dados de arquivos e dados de snapshots para o nível do grupo de capacidade. No entanto, os metadados de arquivos sempre permanecem no nível SSD. Para obter mais informações, consulte Como o armazenamento SSD é usado.

- Automática: essa política move todos os dados frios (dados do usuário e snapshots) para o nível do grupo de capacidade. A taxa de resfriamento dos dados é determinada pelo período de resfriamento da política, cujo padrão é 31 dias, podendo ser configurado para valores entre 2 e 183 dias. Quando os blocos de dados frios subjacentes são lidos aleatoriamente (como no acesso típico a arquivos), eles ficam quentes e são gravados no nível de armazenamento principal. Quando os blocos de dados frios são lidos sequencialmente (por exemplo, por meio de uma verificação do antivírus), eles permanecem frios e no nível de armazenamento do grupo de capacidade. Essa é a política padrão ao criar um volume usando o FSx console da Amazon.
- Somente snapshot: essa política move somente os dados de snapshots para o nível de armazenamento do grupo de capacidade. A taxa na qual os snapshots são divididos em níveis no grupo de capacidade é determinada pelo período de resfriamento da política, cujo padrão é definido como dois dias e pode ser configurado para valores entre 2 e 183 dias. Quando os dados frios do snapshot são lidos, eles ficam quentes e são gravados no nível de armazenamento principal. Essa é a política padrão ao criar um volume usando a FSx API da AWS CLI Amazon ou a CLI do NetApp ONTAP.
- Todos: essa política marca todos os dados do usuário e dados do snapshot como frios e os armazena no nível do grupo de capacidade. Quando os blocos de dados são lidos, eles permanecem frios e não são gravados no nível de armazenamento principal. Quando os dados são gravados em um volume com a política Todos de divisão em níveis, inicialmente, eles ainda são gravados no nível de armazenamento SSD e divididos em níveis no grupo de capacidade por meio de um processo em segundo plano. Se a política All for aplicada a um volume que já contém dados, os dados existentes são escalonados do SSD para o pool de capacidade. Observe que os metadados do arquivo sempre permanecem no nível SSD.
- Nenhum: essa política mantém todos os dados do volume no nível de armazenamento principal e impede que sejam movidos para o armazenamento do grupo de capacidade. Se você definir um volume para essa política depois de usar qualquer outra política, os dados existentes (incluindo instantâneos) no volume que estava no armazenamento do pool de capacidade serão movidos para o armazenamento SSD por um processo em segundo plano. Essa migração de dados ocorre somente quando a utilização do SSD está abaixo de 90% e a política de recuperação da nuvem

está definida como ou. `promote` `on-read` Esse processo em segundo plano pode ser acelerado pela leitura intencional dos dados. Para obter mais informações, consulte Políticas de recuperação na nuvem.

Para obter mais informações sobre como definir ou modificar a política de divisão em níveis de um volume, consulte Atualizar uma política de camadas.

Como prática recomendada, ao migrar dados que planeja armazenar em longo prazo no armazenamento do grupo de capacidade, recomendamos usar a política de divisão Automática em níveis no volume. Com a hierarquização automática, os dados são armazenados no nível de armazenamento SSD por no mínimo 2 dias (com base no período de resfriamento do volume) antes que sejam movidos para o nível do grupo de capacidade. O ONTAP executa periodicamente a desduplicação pós-processo nos dados armazenados no nível de armazenamento SSD, ajustando de modo automático e periódico a frequência com base na taxa de alteração de dados no volume. Taxas mais altas acionam as tarefas de desduplicação pós-processo com maior frequência.

Por padrão, a compactação pós-processo é desabilitada no ONTAP devido ao impacto de desempenho que ela pode ter sobre as workloads em andamento no sistema de arquivos. Antes de habilitar a compactação pós-processo, você deverá avaliar o impacto sobre o desempenho da sua workload. Para habilitar a compactação pós-processo, assuma o nível de privilégio de diagnóstico na CLI do ONTAP e execute o seguinte comando:

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -is-enabled true
```

O ONTAP executa a compressão pós-processamento para dados que estão retidos no armazenamento SSD por no mínimo 14 dias. Para workloads nas quais seja é improvável que os dados sejam acessados após um período mais curto, você pode modificar as configurações de compactação pós-processamento para antecipar a execução da compressão pós-processo. Por exemplo, para aplicar economias de compressão pós-processamento a dados que não tenham sido acessados por 5 dias, execute o seguinte comando da CLI do ONTAP:

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -threshold-days 5 -threshold-days-min 2 -threshold-days-max 14
```

Para obter mais informações sobre o comando, consulte inactive-data-compressionmodificação de eficiência de volume

Ao reter dados em SSD, você maximiza as velocidades de transferência dos backups de volume que você cria, pois as taxas de transferência de dados são mais altas para armazenamento em SSD.

Período de resfriamento da divisão em níveis

O período de resfriamento da divisão em níveis de um volume define o tempo necessário para que os dados no nível SSD sejam marcados como frios. O período de resfriamento se aplica às políticas `Auto` e `Snapshot-only` de divisão em níveis. Você pode definir o período de resfriamento para um valor na faixa de 2 a 183 dias. Para obter mais informações sobre como definir o período de resfriamento, consulte Atualizar o mínimo de dias de resfriamento.

Os dados são divididos em níveis de 24 a 48 horas após o período de resfriamento expirar. A divisão em níveis é um processo em segundo plano que consome recursos da rede e tem uma prioridade menor do que as solicitações voltadas ao cliente. A utilização das atividades de divisão em níveis é controlada quando há solicitações em andamento voltadas ao cliente.

Políticas de recuperação na nuvem

A política de recuperação na nuvem de um volume define as condições que especificam quando os dados lidos no nível do grupo de capacidade podem ser promovidos para o nível SSD. Quando a política de recuperação na nuvem é definida como algo diferente de `Default`, essa política substitui o comportamento de recuperação da política de divisão em níveis do volume. Um volume pode ter uma das políticas de recuperação na nuvem a seguir.

- Padrão: essa política recupera dados divididos em níveis com base na política de divisão em níveis subjacente do volume. Essa é a política padrão de recuperação na nuvem para todos os volumes.
- Nunca: essa política nunca recupera dados divididos em níveis, independentemente de as leituras serem sequenciais ou aleatórias. Isso é semelhante a definir a política de divisão em níveis do volume como Todos, exceto que você pode usá-la com outras políticas, a Automática ou a Somente Snapshot, para dividir os dados de acordo com o período mínimo de resfriamento, em vez de imediatamente.
- Em leitura: essa política recupera os dados divididos em níveis para todas as leituras de dados orientadas pelo cliente. Essa política não tem efeito ao usar a política Todos de divisão em níveis.
- Promover: essa política marca todos os dados de um volume que estão no grupo de capacidade para recuperação no nível SSD. Os dados serão marcados na próxima vez em que o verificador diário de divisão em níveis em segundo plano for executado. Essa política é benéfica para aplicações com workloads cíclicas que são executadas com pouca frequência, mas exigem

performance de nível SSD durante a execução. Essa política não tem efeito ao usar a política Todos de divisão em níveis.

Para obter informações sobre como definir a política de recuperação na nuvem de um volume, consulte Atualizar a política de recuperação na nuvem de um volume.

Limites de divisão em níveis

A utilização da capacidade de armazenamento SSD de um sistema de arquivos determina como o ONTAP gerencia o comportamento de divisão em níveis de todos os volumes. Com base no uso da capacidade de armazenamento SSD de um sistema de arquivos, os seguintes limites definem o comportamento de divisão em níveis conforme descrito. Para obter informações sobre como monitorar a utilização da capacidade do nível de armazenamento SSD de um volume, consulte Monitorar a capacidade de armazenamento de volumes.

> **Note**
>
> Recomendamos que você não exceda 80% da utilização da capacidade de armazenamento do seu nível de armazenamento SSD. Para sistemas de arquivos de segunda geração, essa recomendação se aplica tanto à utilização média total de todos os agregados do sistema de arquivos quanto à utilização de cada agregado individual. Isso garante que a divisão em níveis funcione adequadamente e fornece sobrecarga para novos dados. Se nível de armazenamento SSD estiver consistentemente acima de 80% de utilização da capacidade de armazenamento, você poderá aumentar a capacidade do nível de armazenamento SSD. Para obter mais informações, consulte Atualização do armazenamento SSD e IOPS do sistema de arquivos.

FSx for ONTAP usa os seguintes limites de capacidade de armazenamento para gerenciar a hierarquização em volumes:

- <=50% de utilização do nível de armazenamento SSD: nesse limite, o nível de armazenamento SSD é considerado subutilizado, e somente os volumes que estão usando a política Todos de divisão em níveis têm os dados divididos no armazenamento do grupo de capacidade. Os volumes com as políticas Automática e Somente snapshot não dividem os dados em níveis nesse limite.
- > 50% de utilização do nível de armazenamento SSD: volumes com as políticas Automática e Somente snapshot de divisão em níveis dividem os dados com base na configuração de dias mínimos de resfriamento dos níveis. A configuração padrão é de 31 dias.

- >= 90% de utilização do nível de armazenamento SSD — Nesse limite, a FSx Amazon prioriza a preservação do espaço no nível de armazenamento SSD. Os dados frios do nível do grupo de capacidade não são mais movidos para o nível de armazenamento SSD quando lidos em volumes usando as políticas Automática e Somente snapshot.
- >=98% de utilização do nível de armazenamento SSD: toda a funcionalidade de divisão em níveis é interrompida quando o nível de armazenamento SSD atinge ou ultrapassa 98% de utilização. Você pode continuar lendo nos níveis de armazenamento, mas não é possível gravar neles.

Snapshots e capacidade de armazenamento de volumes

Um snapshot é uma imagem somente para leitura de um volume Amazon FSx for NetApp ONTAP em um determinado momento. Os snapshots oferecem proteção contra exclusão ou modificação acidental de arquivos nos volumes. Com os snapshots, seus usuários podem facilmente visualizar e restaurar arquivos individuais ou pastas de um snapshot anterior.

Os snapshots são armazenados com os dados do sistema de arquivos e consomem a capacidade de armazenamento do sistema de arquivos. No entanto, os snapshots consomem capacidade de armazenamento somente para as partes dos arquivos que foram alteradas após o último snapshot. Os snapshots não estão incluídos nos backups dos volumes do sistema de arquivos.

Os snapshots são habilitados por padrão nos volumes, usando a política de snapshots padrão. Os snapshots são armazenados no diretório `.snapshot` na raiz de um volume. Você pode gerenciar a capacidade de armazenamento de um volume para snapshots das maneiras a seguir.

- Políticas de snapshot: selecione uma política de snapshot incorporada ou uma política personalizada criada na CLI ou na API REST do ONTAP.
- Excluir os snapshots manualmente: recupere a capacidade de armazenamento excluindo os snapshots manualmente.
- Criar uma política de exclusão automática de snapshot: crie uma política que exclua mais snapshots do que a política de snapshot padrão.
- Desativar os snapshots automáticos: conserve a capacidade de armazenamento desativando os snapshots automáticos.

Para obter mais informações, consulte Como proteger seus dados com snapshots.

Capacidade do arquivo de volumes

Os volumes Amazon FSx for NetApp ONTAP têm ponteiros de arquivo que são usados para armazenar metadados de arquivos, como nome do arquivo, horário do último acesso, permissões, tamanho e para servir como ponteiros para blocos de dados. Esses ponteiros de arquivo são chamados de inodes. Cada volume tem uma capacidade finita para o número de inodes, que é chamada de capacidade do arquivo de volumes. Quando um volume fica com poucos arquivos disponíveis (inodes) ou os esgota, você não consegue gravar dados adicionais nesse volume.

O número de objetos do sistema de arquivos (arquivos, diretórios, cópias de snapshots) que um volume pode conter é determinado pela quantidade de inodes que ele tem. O número de inodes em um volume aumenta proporcionalmente à capacidade de armazenamento do volume (e ao número de componentes de volume para volumes do FlexGroup). Por padrão, volumes do FlexVol (ou constituintes do FlexGroup) com uma capacidade de armazenamento de 648 GiB ou mais têm o mesmo número de inodes: 21.251.126. Se você criar um volume maior que 648 GiB e quiser que ele tenha mais de 21.251.126 inodes, deverá aumentar o número máximo de inodes (arquivos) manualmente. Para obter mais informações sobre como visualizar o número máximo de arquivos de um volume, consulte Monitorar a capacidade de arquivos de um volume.

O número padrão de inodes em um volume é de 1 inode para cada 32 KiB de capacidade de armazenamento de volume, até um tamanho de volume de 648 GiB. Para um volume de 1 GiB:

Volume_size_in_bytes × (1 arquivo ÷ inode_size_in_bytes) = maximum_number_of_files

1.073.741.824 bytes × (1 arquivo ÷ 32.768 bytes) = 32.768 arquivos

Você pode aumentar o número máximo de inodes que um volume pode conter, até um máximo de 1 inode para cada 4 KiB de capacidade de armazenamento. Para um volume de 1 GiB, isso aumenta o número máximo de inodes ou arquivos de 32.768 para 262.144:

1.073.741.824 bytes × (1 arquivo ÷ 4.096 bytes) = 262.144 arquivos

E FSx para o volume ONTAP pode ter no máximo 2 bilhões de inodes.

Para obter informações sobre como alterar o número máximo de arquivos que um volume pode armazenar, consulte Atualizar o número máximo de arquivos em um volume.

Como gerenciar eficiências de armazenamento

Ao permitir a eficiência do armazenamento em seus FSx volumes do ONTAP, você pode otimizar a utilização do armazenamento, reduzir os custos de armazenamento e melhorar o desempenho geral do seu sistema de arquivos.

ONTAPorganiza os arquivos em blocos de dados de 4 kibibytes (KiB). A eficiência do armazenamento ocorre no nível do bloco de dados e não no nível dos arquivos individuais. Quando as eficiências de armazenamento estiverem habilitadas, o ONTAP emprega uma combinação de técnicas de redução de dados para eliminar dados duplicados, compactar o tamanho dos dados e reorganizar o layout dos dados para otimizar o uso do disco.

A eficiência do armazenamento é aplicada de duas maneiras. Elas são aplicadas aos dados em linha (na memória, antes da gravação dos dados em disco) para proporcionar economia imediata de armazenamento. Elas também são aplicadas aos dados em segundo plano (após a gravação dos dados em disco) na camada de armazenamento SSD por meio de trabalhos periódicos de eficiência para otimizar a utilização do armazenamento ao longo do tempo. As eficiências de armazenamento em segundo plano não funcionam nos dados depois que eles são hierarquizados no grupo de capacidade. No entanto, se os dados tivessem alguma economia de armazenamento enquanto estavam no SSD, essa economia será preservada quando os dados forem hierarquizados no grupo de capacidade.

> **Note**
>
> O ONTAP não é compatível com a habilitação de eficiências de armazenamento em volumes de proteção de dados (DP). No entanto, a economia de armazenamento obtida no volume leitura-gravável (RW) de origem é preservada quando os dados são replicados para o volume DP de destino.

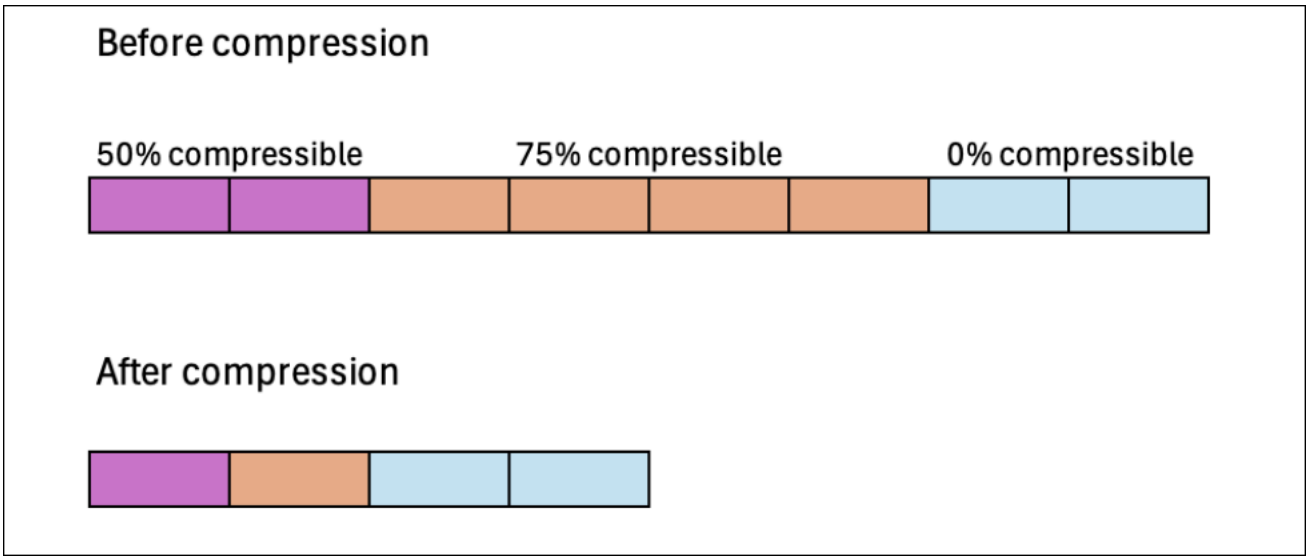
Compressão de blocos de dados

Grupos de compressão são agrupamentos lógicos de dados que são gerenciados e comprimidos juntamente como um único bloco. O ONTAP empacota automaticamente os blocos de dados em grupos de compressão, o que reduz o espaço consumido em disco. Para otimizar o desempenho e a utilização do armazenamento, o ONTAP disponibiliza uma abordagem equilibrada para gerenciar dados ajustando o grau de compressão aplicado aos dados com base em seus padrões de acesso.

Por padrão, os dados são comprimidos em linha usando grupos de compressão de 8 KB para garantir o desempenho ideal ao gravar dados em um volume. Opcionalmente, você pode aplicar uma compressão mais pesada aos dados ativando a compressão de dados inativos em um volume para comprimir ainda mais os dados no SSD. A compressão de dados inativos usa grupos de compressão de 32 KB em dados frios para economizar ainda mais no armazenamento. Para obter mais informações, consulte o comando `volume efficiency inactive-data-compression modify` na NetApp ONTAP Documentation Center.

> **Note**
>
> A compactação de dados inativos consome IOPS adicionais de CPU e disco, e pode ser uma tarefa que consome muitos recursos. Recomendamos que você avalie o impacto no desempenho da execução da compactação de dados inativos em sua workloads antes de ativar esse recurso.

A imagem a seguir ilustra a economia de armazenamento que pode ser obtida com a compressão de blocos de dados.



Desduplicação de blocos de dados

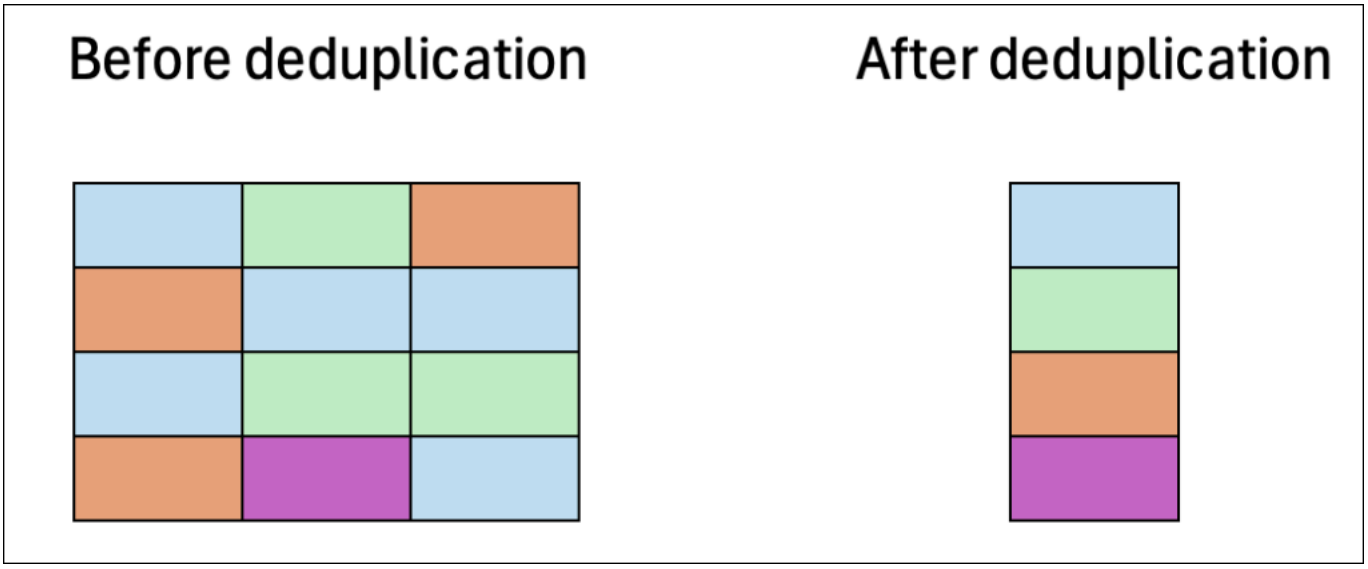
O ONTAP detecta e elimina blocos de dados duplicados para reduzir redundâncias nos dados. Os blocos duplicados são substituídos por referências a blocos exclusivos compartilhados.

Por padrão, os dados são desduplicados em linha para reduzir o espaço de armazenamento antes da gravação em disco. O ONTAP também executa uma varredura de desduplicação em segundo

plano em intervalos especificados para identificar e eliminar dados duplicados após a gravação no disco. Durante essas verificações agendadas, o ONTAP processa um registro de alterações para identificar blocos de dados novos ou modificados desde a última verificação que ainda não foram desduplicados. Ao encontrar duplicatas, o ONTAP atualiza os metadados para apontar para uma única cópia dos blocos duplicados e marca os blocos redundantes como espaço livre pronto para ser recuperado.

> **Note**
>
> O ONTAP aplica a desduplicação a 4 KB de gravações recebidas por vez, então você pode ver uma economia menor de desduplicação ao executar workloads com gravações menores que 4 KB de tamanho.
> FSx for ONTAP não oferece suporte à desduplicação entre volumes.

A imagem a seguir ilustra as economias de armazenamento que podem ser obtidas com a desduplicação.

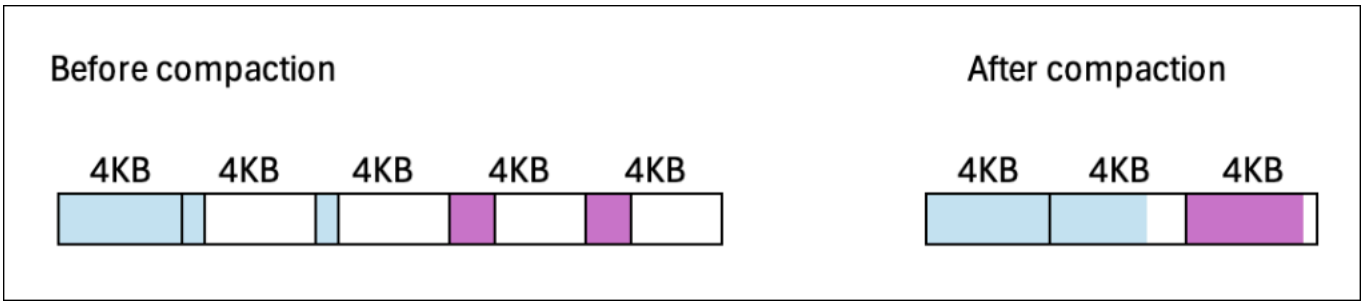


Compactação de blocos de dados

O ONTAP consolida blocos de dados parcialmente preenchidos com menos de 4 KB cada em um bloco de 4 KB utilizado com mais eficiência.

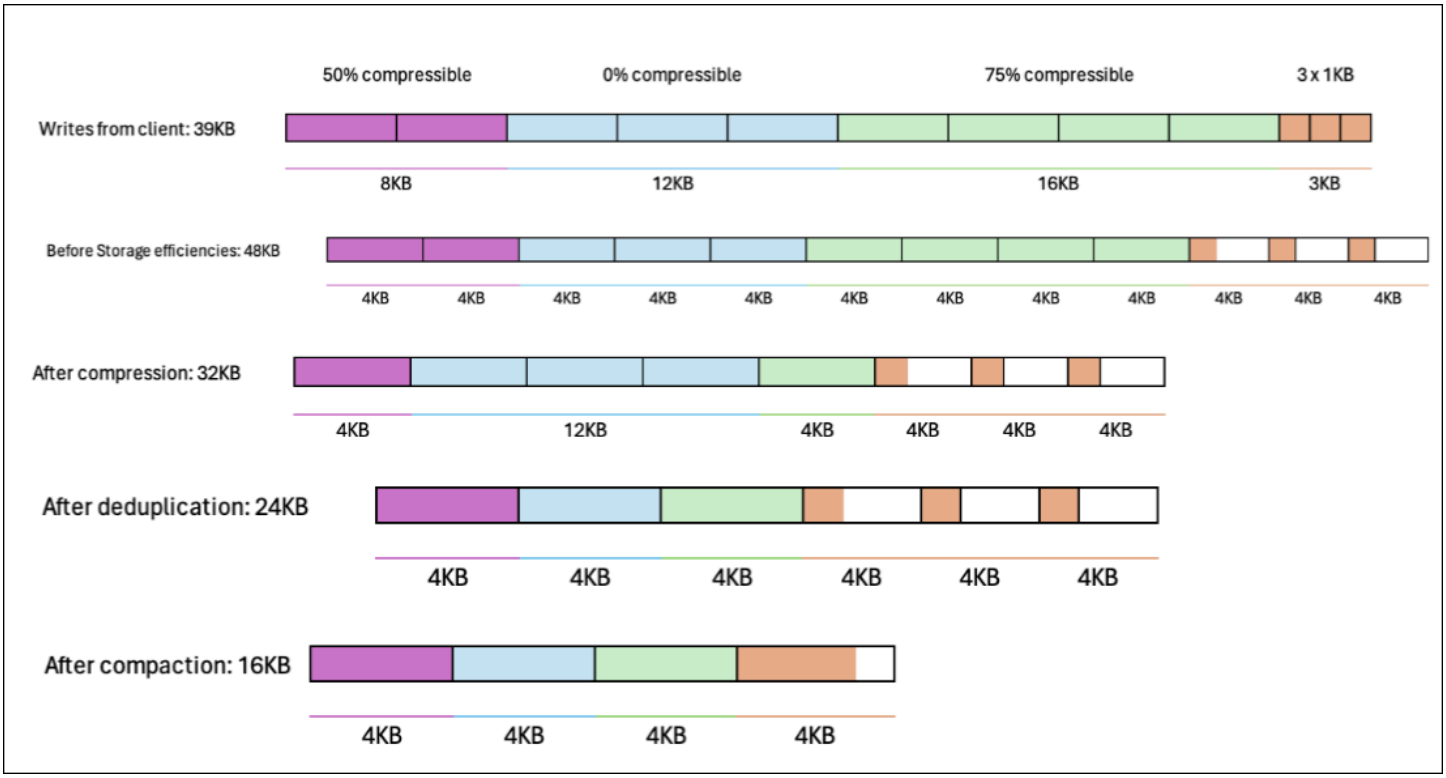
Por padrão, os dados são compactados em linha para otimizar o layout dos dados conforme eles são gravados em disco a fim de minimizar a sobrecarga de armazenamento, reduzir a fragmentação e melhorar o desempenho de leitura.

A imagem a seguir ilustra as economias de armazenamento que podem ser obtidas com a compactação.



Exemplo: eficiências de armazenamento

A imagem a seguir ilustra como as eficiências de armazenamento são aplicadas aos dados.



Habilitar o dimensionamento automático

Dimensionamento automático do volume para que ele aumente automaticamente até um tamanho especificado quando atingir um limite de espaço usado. Você pode fazer isso para tipos de FlexVol volume (o tipo de volume padrão FSx para ONTAP) usando o comando `volume autosize`ONTAP CLI.

Habilitar o dimensionamento automático de volumes (CLI do ONTAP)

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Use o comando `volume autosize` conforme mostrado a seguir, substituindo também os valores.

   - Substitua *svm_name* pelo nome da SVM na qual o volume foi criado.
   - Substitua *vol_name* pelo nome do volume que deseja redimensionar.
   - Substitua *grow_threshold* por um valor percentual de espaço usado (como `90`) no qual o volume aumentará automaticamente de tamanho (até o valor *max_size*).
   - Substitua *max_size* pelo tamanho máximo até o qual o volume pode aumentar. Use o formato *integer*`[KB|MB|GB|TB|PB]`; por exemplo, `300TB`. O tamanho máximo é de 300 TB. O padrão é 120% do tamanho do volume.
   - *min_size*Substitua pelo tamanho mínimo para o qual o volume diminuirá. Use o mesmo formato de*max_size*.
   - *shrink_threshold*Substitua pela porcentagem de espaço usado na qual o volume diminuirá automaticamente de tamanho.

   ```
   ::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -
   grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-
   percent shrink_threshold -minimum-size min_size
   ```

3. Para mostrar a configuração atual de tamanho automático, execute o comando a seguir. Substitua *svm_name* e *vol_name* por suas informações.

   ```
   ::> volume autosize -vserver svm_name -volume vol_name
   ```

Habilitar o modo de gravação na nuvem

Use o comando `volume modify` da CLI do ONTAP para habilitar ou desabilitar o modo de gravação na nuvem de um volume existente. Para obter mais informações, consulte o Centro `volume modify`de Documentação do NetApp ONTAP.

Os pré-requisitos para definir o modo de gravação na nuvem são:

- O volume deve ser um volume existente. Você só pode habilitar o recurso em um volume existente.
- O volume deve ser um volume de leitura/gravação (RW).
- O volume deve ter a política de camadas All. Para obter mais informações sobre como modificar a política de camadas de um volume, consulte Atualizar uma política de camadas.

O modo de gravação na nuvem é útil para casos como migrações (por exemplo, quando grandes quantidades de dados são transferidas para um sistema de arquivos usando o protocolo NFS).

Definir o modo de gravação na nuvem de um volume (CLI do ONTAP)

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Entre no modo avançado da CLI do ONTAP usando o comando a seguir.

   ```
   FSx::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Use o comando a seguir para definir o modo de gravação na nuvem do volume, substituindo os seguintes valores:

   - Substitua *`svm_name`* pelo nome da SVM na qual o volume foi criado.

- Substitua *vol_name* pelo nome do volume para o qual está definindo o modo de gravação na nuvem.
- Substitua *vol_cw_mode* por `true` para habilitar o modo de gravação na nuvem no volume ou por `false` para desabilitá-lo.

```
FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-
enabled vol_cw_mode
```

O sistema responde da seguinte forma para uma solicitação bem-sucedida:

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Como atualizar a capacidade de armazenamento

Você pode gerenciar a capacidade de armazenamento de volume aumentando ou diminuindo manualmente o tamanho do volume usando a API AWS Management Console, AWS CLI e a CLI do ONTAP. Você também pode habilitar o dimensionamento automático do volume para que seu tamanho aumente ou diminua automaticamente quando atingir determinados limites de capacidade de armazenamento usada. Use a CLI do ONTAP para gerenciar o dimensionamento automático de volumes.

Alterar a capacidade de armazenamento de um volume (console)

- Você pode aumentar ou diminuir a capacidade de armazenamento de um volume usando o FSx console e a API da Amazon. AWS CLI Para obter mais informações, consulte Atualizar volumes.

Você também pode usar a CLI do ONTAP para modificar a capacidade de armazenamento de um volume usando o comando `volume modify`.

Modificar o tamanho de um volume (CLI do ONTAP)

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Use o comando volume modify da CLI do ONTAP para modificar a capacidade de armazenamento de um volume. Execute o seguinte comando, usando seus dados no lugar dos seguintes valores:

   - Substitua *svm_name* pelo nome da máquina virtual de armazenamento (SVM) na qual o volume foi criado.
   - Substitua *vol_name* pelo nome do volume que deseja redimensionar.
   - Substitua *vol_size* pelo novo tamanho do volume no formato *integer*[KB|MB|GB|TB|PB]; por exemplo, 100GB para aumentar o tamanho do volume para 100 gigabytes.

```
::> volume modify -vserver svm_name -volume vol_name -size vol_size
```

Atualizar uma política de camadas

Você pode modificar a política de classificação por níveis de um volume usando a API AWS Management Console, AWS CLI e a CLI do ONTAP.

Modificar a política de camadas de dados de um volume (console)

Use o procedimento a seguir para modificar a política de divisão de dados em níveis de um volume usando o AWS Management Console.

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Escolha Volumes no painel de navegação à esquerda e selecione o volume do ONTAP para o qual você deseja modificar a política de divisão de dados em níveis.
3. Escolha Atualizar volume no menu suspenso Ações. A janela Atualizar volume é exibida.
4. Em Política de divisão em níveis do grupo de capacidade, escolha a nova política para o volume. Para obter mais informações, consulte Políticas de camadas de volume.
5. Escolha Atualizar para aplicar a nova política ao volume.

Definir a política de camadas de um volume (CLI)

- Modifique a política de classificação por níveis de um volume usando o comando da CLI update-volume (UpdateVolumeé a ação equivalente da API da Amazon FSx). O exemplo de comando da CLI a seguir define a política de divisão de dados em níveis de um volume como SNAPSHOT_ONLY.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

Para uma solicitação bem-sucedida, o sistema responde com a descrição do volume.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 2,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

Modificar a política de camadas de um volume (CLI do ONTAP)

Use o comando `volume modify` da CLI do ONTAP para definir a política de divisão em níveis de um volume. Para obter mais informações, consulte o Centro `volume modify`de Documentação do NetApp ONTAP.

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Entre no modo avançado da CLI do ONTAP usando o comando a seguir.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Use o comando a seguir para modificar a política de divisão de dados em níveis do volume, substituindo também os valores.

   - Substitua *`svm_name`* pelo nome da SVM na qual o volume foi criado.
   - Substitua *`vol_name`* pelo nome do volume para o qual você está definindo a política de divisão de dados em níveis.
   - Substitua *`tiering_policy`* pela política desejada. Os valores válidos são `snapshot-only`, `auto`, `all` ou none. Para obter mais informações, consulte Políticas de camadas de volume.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -tiering-
   policy tiering_policy
   ```

Atualizar o mínimo de dias de resfriamento

Os dias mínimos de resfriamento de um volume definem o limite usado para determinar quais dados estão quentes e quais estão frios. Você pode definir os dias mínimos de resfriamento de um volume usando uma API AWS CLI e a CLI do ONTAP.

Definir os dias mínimos de resfriamento de um volume (CLI)

- Modifique uma configuração de volume usando o comando update-volume CLI (é a ação equivalente UpdateVolumeda API da Amazon FSx). O exemplo a seguir de comando da CLI define o `CoolingPeriod` de um volume para 104 dias.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration
 TieringPolicy={CoolingPeriod=104}
```

O sistema responde com a descrição do volume para uma solicitação bem-sucedida.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 104,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
```

```
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

Definir os dias mínimos de resfriamento de um volume (CLI do ONTAP)

Use o comando `volume modify` da CLI do ONTAP para definir o número mínimo de dias de resfriamento para um volume existente. Para obter mais informações, consulte o Centro `volume modify`de Documentação do NetApp ONTAP.

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Entre no modo avançado da CLI do ONTAP usando o comando a seguir.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Use o comando a seguir para alterar os dias mínimos de resfriamento da divisão em níveis do volume, substituindo também valores.

   - Substitua *`svm_name`* pelo nome da SVM na qual o volume foi criado.
   - Substitua *`vol_name`* pelo nome do volume para o qual você está definindo os dias de resfriamento.
   - Substitua *`cooling_days`* pelos dias desejados, um número inteiro entre 2 e 183.

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-
days cooling_days
```

O sistema responde da seguinte forma para uma solicitação bem-sucedida:

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Atualizar a política de recuperação na nuvem de um volume

Use o comando `volume modify` da CLI do ONTAP para definir a política de recuperação na nuvem de um volume existente. Para obter mais informações, consulte o Centro `volume modify`de Documentação do NetApp ONTAP.

Definir a política de recuperação na nuvem de um volume (CLI do ONTAP)

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Entre no modo avançado da CLI do ONTAP usando o comando a seguir.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Use o comando a seguir para definir a política de recuperação na nuvem do volume, substituindo também os valores.

   - Substitua *svm_name* pelo nome da SVM na qual o volume foi criado.

- Substitua *vol_name* pelo nome do volume para o qual você está definindo a política de recuperação na nuvem.
- Substitua *retrieval_policy* pelo valor desejado, `default`, `on-read`, `never` ou `promote`.

```
FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-
policy retrieval_policy
```

O sistema responde da seguinte forma para uma solicitação bem-sucedida:

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Atualizar o número máximo de arquivos em um volume

FSx para ONTAP, os volumes podem ficar sem capacidade de arquivo quando o número de inodes ou ponteiros de arquivo disponíveis estiver esgotado.

Aumentar o número máximo de arquivos em um volume (CLI do ONTAP)

Use o comando `volume modify` da CLI do ONTAP para aumentar o número máximo de arquivos em um volume. Para obter mais informações, consulte `volume modify` na Central de documentação do NetApp ONTAP.

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.
2. Faça um dos procedimentos a seguir, dependendo do seu caso de uso. Substitua *svm_name* e *vol_name* pelos seus valores.

   - Para configurar um volume para sempre ter o número máximo de arquivos (inodes) disponíveis, siga os passos a seguir.

1. Entre no modo avançado na CLI do ONTAP usando o comando a seguir.

```
::> set adv
```

2. Após executar esse comando, você verá essa saída. Insira y para continuar.

```
Warning: These advanced commands are potentially dangerous; use them only
 when
directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

3. Insira o seguinte comando para sempre usar o número máximo de arquivos no volume:

```
::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
```

- Para especificar manualmente o número total de arquivos permitidos no volume, usando *max_number_files* = (current_size_of_volume) × (1 file ÷ 4 KiB), com um valor máximo possível de dois bilhões, use o seguinte comando:

```
::> volume modify -vserver svm_name -volume vol_name -files max_number_files
```

Monitorar a capacidade de armazenamento de volumes

Você pode visualizar o armazenamento disponível de um volume e sua distribuição de armazenamento no AWS Management Console AWS CLI, e na CLI do NetApp ONTAP.

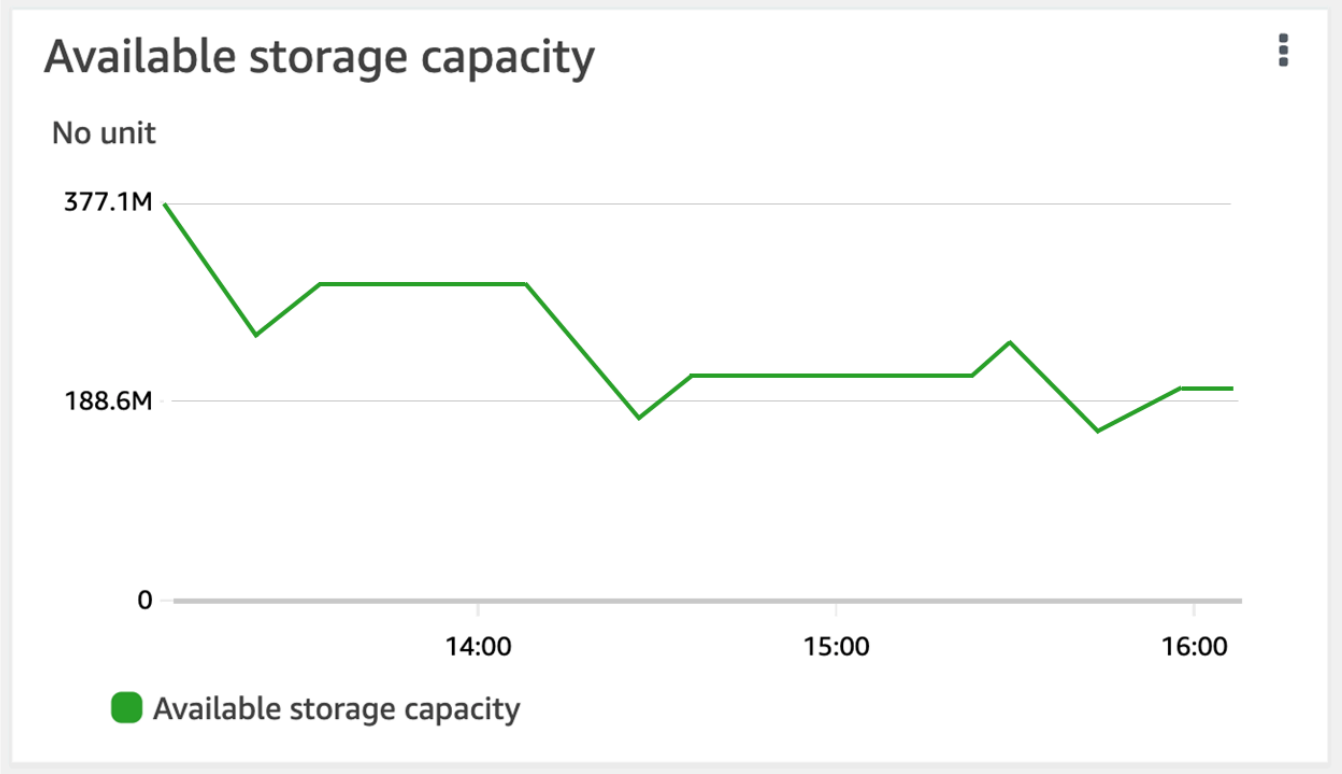
Monitorar a capacidade de armazenamento de um volume (console)

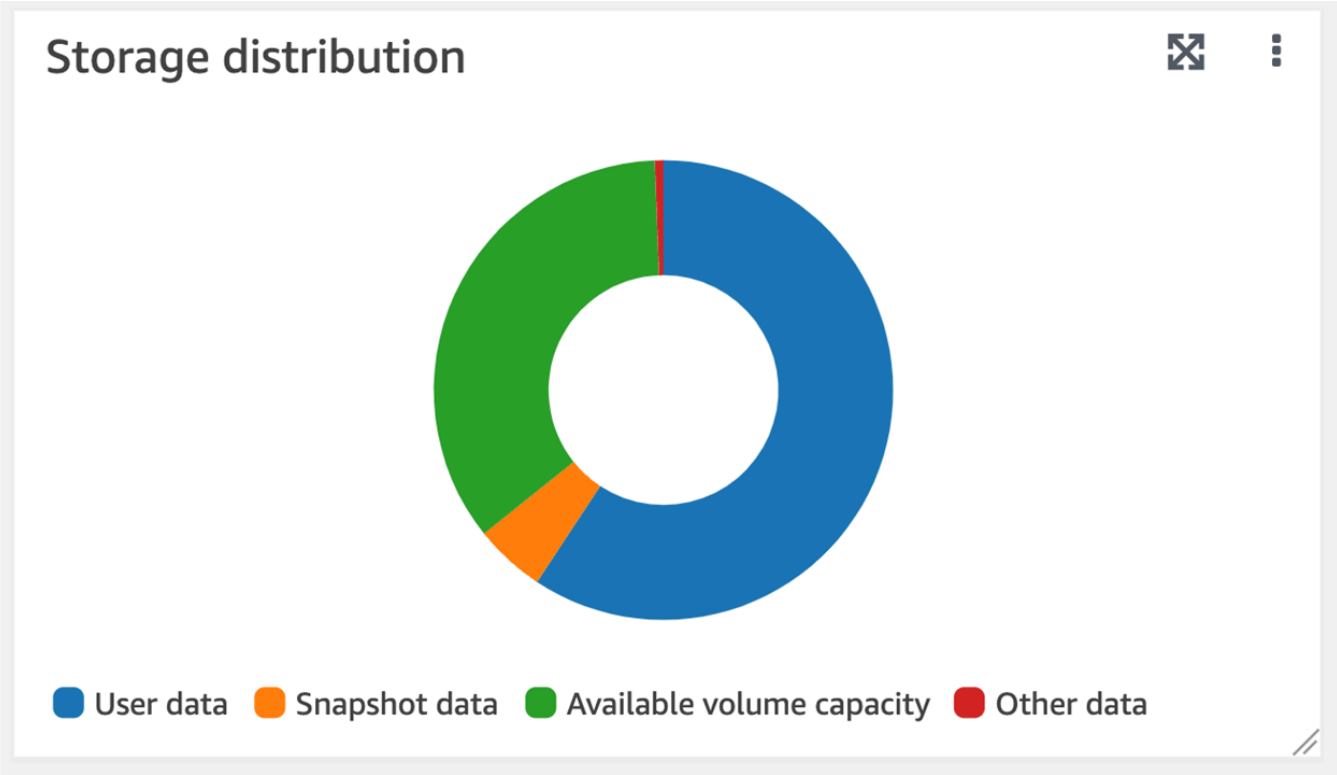
O gráfico Armazenamento disponível exibe a quantidade de capacidade de armazenamento livre em um volume ao longo do tempo. O gráfico Distribuição do armazenamento mostra como a capacidade de armazenamento de um volume está atualmente distribuída em quatro categorias:

- Dados do usuário
- Dados de snapshot
- Capacidade de volume disponível
- Outros dados

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.

2. Escolha Volumes na coluna de navegação à esquerda e selecione o volume do ONTAP para o qual deseja visualizar as informações sobre a capacidade de armazenamento. A página de detalhes do volume é exibida.
3. No segundo painel, escolha a guia Monitoramento. Os gráficos Armazenamento disponível e Distribuição do armazenamento são exibidos com vários outros gráficos.





Monitorar a capacidade de armazenamento de um volume (CLI do ONTAP)

Você pode monitorar como a capacidade de armazenamento do volume está sendo consumida usando o comando `volume show-space` da CLI do ONTAP. Para obter mais informações, consulte `volume show-space` na Central de documentação do NetApp ONTAP.

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Visualize o uso da capacidade de armazenamento de um volume emitindo o comando a seguir, substituindo também os valores.

   - Substitua *`svm_name`* pelo nome da SVM na qual o volume foi criado.

- Substitua *vol_name* pelo nome do volume para o qual você está definindo a política de divisão de dados em níveis.

```
::> volume show-space -vserver svm_name -volume vol_name
```

Se o comando for bem-sucedido, você verá uma saída semelhante a esta:

```
Vserver : svm_name
Volume  : vol_name
Feature                                     Used      Used%
--------------------------------     ----------     ------
User Data                                  140KB         0%
Filesystem Metadata                      164.4MB         1%
Inodes                                   10.28MB         0%
Snapshot Reserve                         563.2MB         5%
Deduplication                               12KB         0%
Snapshot Spill                            9.31GB        85%
Performance Metadata                        668KB         0%

Total Used                               10.03GB        91%

Total Physical Used                      10.03GB        91%
```

A saída desse comando mostra a quantidade de espaço físico que diferentes tipos de dados ocupam nesse volume. Também mostra a porcentagem da capacidade total do volume que cada tipo de dado consome. Nesse exemplo, `Snapshot Spill` e `Snapshot Reserve` consomem um total de 90% da capacidade do volume.

`Snapshot Reserve` mostra a quantidade de espaço em disco reservada para armazenar cópias de snapshot. Se o armazenamento das cópias de snapshot exceder o espaço de reserva, ele será vazado para o sistema de arquivos e essa quantidade será mostrada em `Snapshot Spill`.

Para aumentar a quantidade de espaço disponível, você pode aumentar o tamanho do volume ou excluir snapshots que não está usando, conforme mostrado nos procedimentos a seguir.

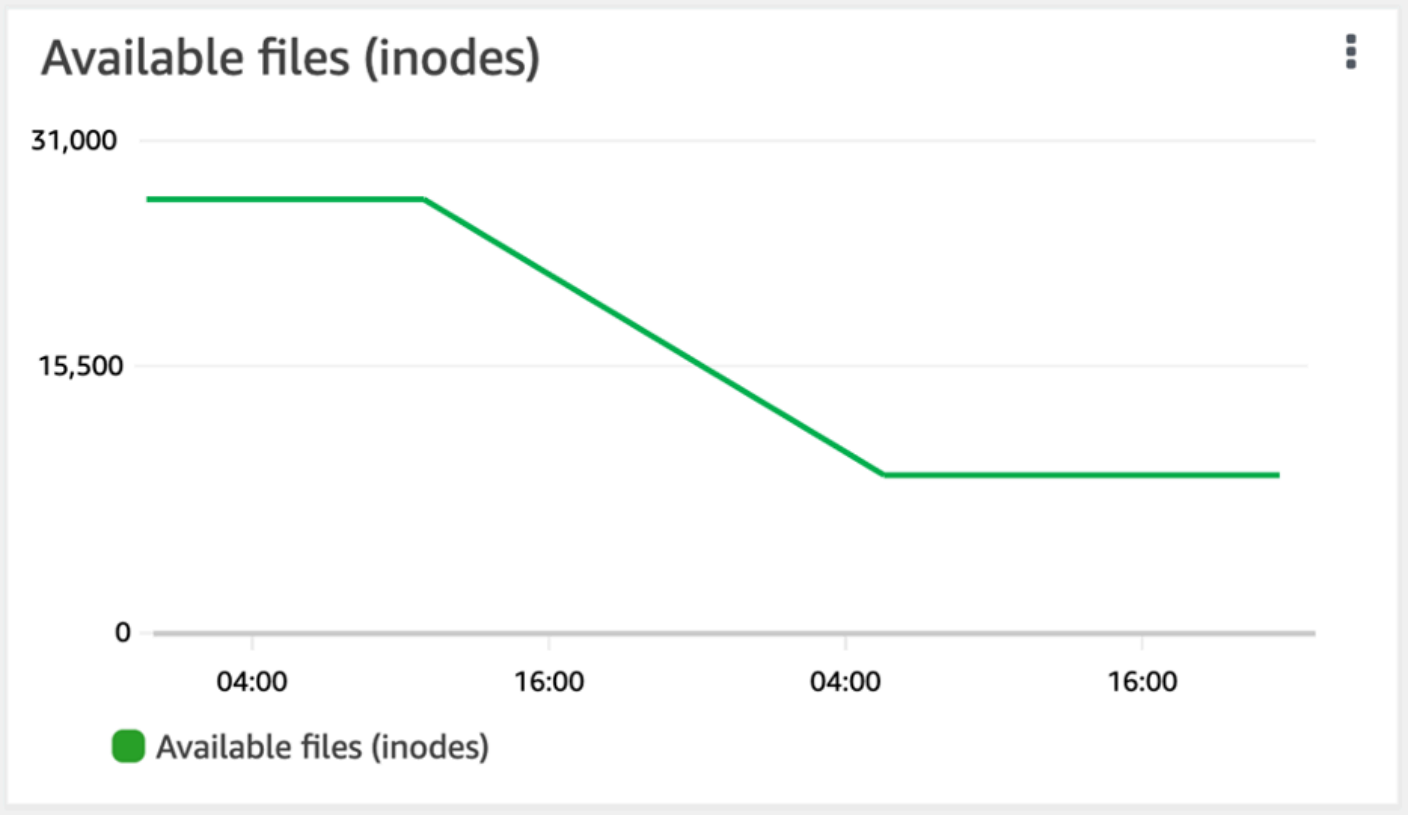
Para tipos de FlexVol volume (o tipo de volume padrão FSx para volumes ONTAP), você também pode ativar o dimensionamento automático de volume. Ao habilitar o dimensionamento automático,

o tamanho do volume aumenta automaticamente quando atinge determinados limites. Você também pode desabilitar os snapshots automáticos. Esses dois recursos são explicados nas seções a seguir.

Monitorar a capacidade de arquivos de um volume

Você pode usar qualquer um dos métodos a seguir para visualizar o número máximo de arquivos permitidos e o número de arquivos já usados em um volume.

- As métricas de CloudWatch volume `FilesCapacity` `FilesUsed` e.
- No FSx console da Amazon, navegue até o gráfico Arquivos disponíveis (inodes) na guia Monitoramento do seu volume. A imagem a seguir mostra os Arquivos disponíveis (inodes) em um volume diminuindo com o tempo.



Gerenciamento FSx para sistemas de arquivos ONTAP

Um sistema de arquivos é o principal FSx recurso da Amazon, análogo a um cluster ONTAP local. Você especifica a capacidade do armazenamento SSD e a capacidade de throughput do seu sistema de arquivos e escolhe uma nuvem privada virtual (VPC) na qual criar o sistema de arquivos. Cada

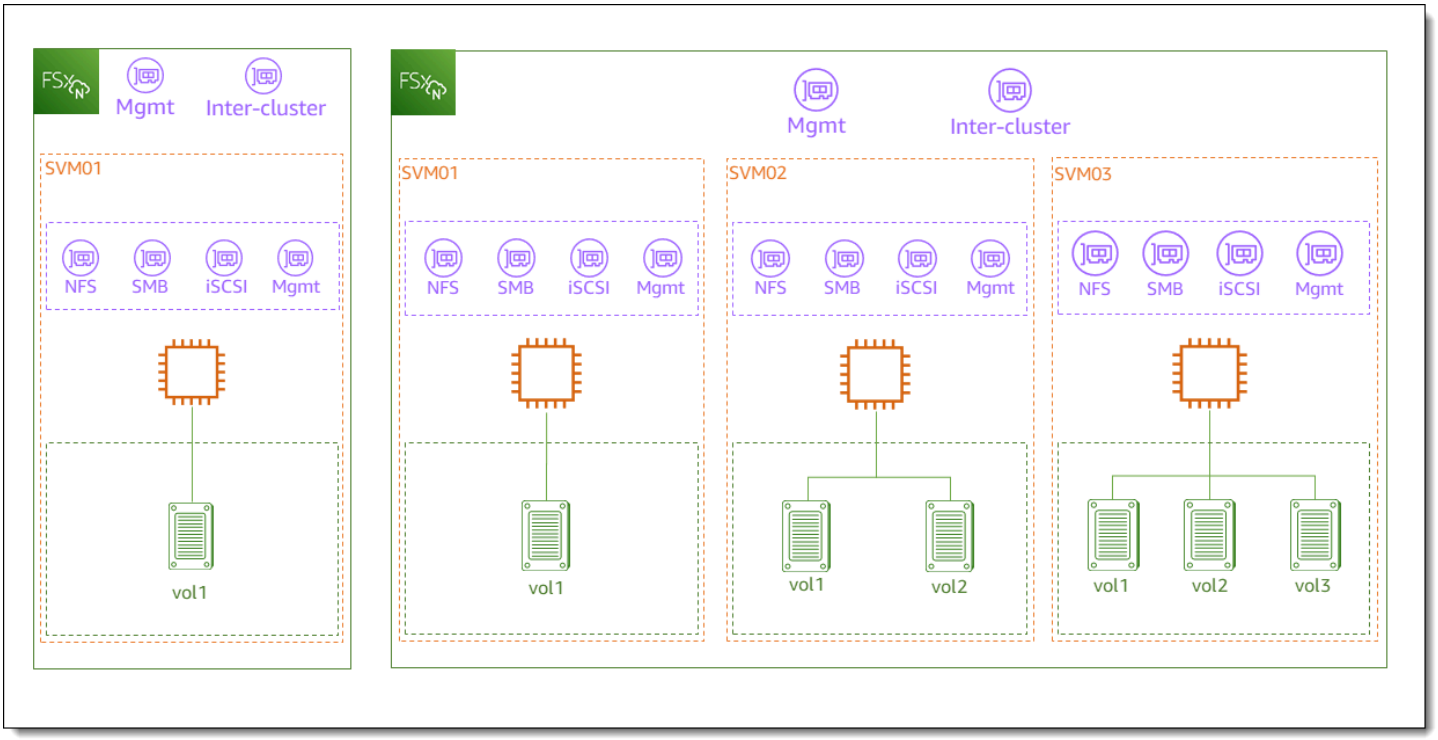
sistema de arquivos tem um endpoint de gerenciamento que você pode usar para gerenciar recursos e dados com a API REST ou a CLI do ONTAP.

Recursos do sistema de arquivos

Um sistema de arquivos Amazon FSx for NetApp ONTAP é composto pelos seguintes recursos principais:

- O hardware físico do próprio sistema de arquivos, que inclui os servidores de arquivos e a mídia de armazenamento.
- Um ou mais pares de servidores de arquivos de alta disponibilidade (HA), que hospedam suas máquinas virtuais de armazenamento ()SVMs. Os sistemas de arquivos de primeira geração e os sistemas de arquivos Multi-AZ de segunda geração têm um par de HA, e os sistemas de arquivos Single-AZ de segunda geração têm até 12 pares de HA. Cada par de HA tem um grupo de armazenamento chamado agregado. A coleção de agregados em todos os pares de HA compõe o seu nível de armazenamento SSD.
- Um ou mais SVMs que hospedam os volumes do sistema de arquivos e têm suas próprias credenciais e gerenciamento de acesso.
- Um ou mais volumes que organizam virtualmente seus dados e são montados por seus clientes.

A imagem a seguir ilustra a arquitetura de um sistema de arquivos ONTAP de primeira geração FSx com um par de HA e a relação entre seus recursos principais. O sistema de arquivos FSx for ONTAP à esquerda é o sistema de arquivos mais simples, com um SVM e um volume. O sistema de arquivos à direita tem vários SVMs, com alguns SVMs com vários volumes. SVMs Cada um dos sistemas de arquivos tem vários endpoints de gerenciamento e SVMs também tem endpoints de acesso a dados.



Ao criar um sistema de arquivos FSx para ONTAP, você define as seguintes propriedades:

- Tipo de implantação: o tipo de implantação do seu sistema de arquivos (várias AZs ou uma única AZ). Os sistemas de arquivos single-AZ replicam os dados e oferecem failover automático em uma única zona de disponibilidade. Os sistemas de arquivos Single-AZ de primeira geração são compatíveis com um par de HA. Os sistemas de arquivos Single-AZ de segunda geração são compatíveis com até 12 pares de HA. Os sistemas de arquivos com várias AZs oferecem maior resiliência ao também replicar seus dados e oferecer suporte ao failover em várias zonas de disponibilidade dentro da mesma Região da AWS. Os sistemas de arquivos Multi-AZ de primeira e segunda geração são compatíveis com um par de HA.

> **Note**
>
> Você não pode alterar o tipo de implantação do sistema de arquivos após a criação. Se quiser alterar o tipo de implantação (por exemplo, passar da Single-AZ 1 para a Single-AZ 2), você poderá fazer backup dos dados e restaurá-los em um novo sistema de arquivos. Você também pode migrar seus dados com NetApp SnapMirror AWS DataSync, com ou com uma ferramenta de cópia de dados de terceiros. Para obter mais informações, consulte Migrando FSx para o ONTAP usando NetApp SnapMirror e Migrando FSx para o ONTAP usando AWS DataSync.

- Capacidade de armazenamento: a quantidade de armazenamento SSD, com até 192 tebibytes (TiB) para sistemas de arquivos de primeira geração, 512 TiB para sistemas de arquivos Multi-AZ de segunda geração e 1 pebibyte (PiB) para sistemas de arquivos Single-AZ de segunda geração.
- IOPS de SSD: por padrão, cada gigabyte de armazenamento SSD inclui três IOPS de SSD (até o máximo atendido pela configuração do sistema de arquivos). Você tem a opção de provisionar IOPS de SSD adicionais conforme necessário.
- Capacidade de throughput: a velocidade sustentada na qual o servidor de arquivos pode fornecer dados.
- Rede: a VPC e as sub-redes para os endpoints de gerenciamento e de acesso a dados que o sistema de arquivos cria. Para um sistema de arquivos com várias AZs, você também define um intervalo de endereços IP e tabelas de rotas.
- Criptografia — A chave AWS Key Management Service (AWS KMS) usada para criptografar os dados do sistema de arquivos em repouso.
- Acesso administrativo: você pode especificar a senha do usuário `fsxadmin`. Você pode usar esse usuário para administrar o sistema de arquivos usando a NetApp CLI e a API REST do ONTAP.

Você pode gerenciar os sistemas FSx de arquivos ONTAP usando a NetApp CLI do ONTAP ou a API REST. Você também pode configurar SnapMirror ou SnapVault relacionar um sistema de FSx arquivos da Amazon e outra implantação do ONTAP (incluindo outro sistema de FSx arquivos da Amazon). Cada sistema FSx de arquivos do ONTAP tem os seguintes endpoints do sistema de arquivos que fornecem acesso aos NetApp aplicativos:

- Gerenciamento — Use esse endpoint para acessar a NetApp CLI do ONTAP via Secure Shell (SSH) ou para usar a API REST do NetApp ONTAP com seu sistema de arquivos.
- Intercluster — Use esse endpoint ao configurar o uso da replicação NetApp SnapMirror ou do armazenamento em cache. NetApp FlexCache

Para obter mais informações, consulte Gerenciando FSx recursos do ONTAP usando NetApp aplicações e Replicando seus dados usando NetApp SnapMirror.

Criar sistemas de arquivos

Esta seção descreve como criar um sistema de arquivos FSx para ONTAP usando o FSx console da Amazon ou a FSx API da Amazon. AWS CLI Você pode criar um sistema de arquivos em uma nuvem privada virtual (VPC) de sua propriedade ou em uma VPC que outra pessoa Conta da AWS

compartilhou com você. É necessário considerar alguns fatores ao criar um sistema de arquivos Multi-AZ em uma VPC que você participa. Esses fatores são apresentados neste tópico.

Por padrão, quando você cria um novo sistema de arquivos a partir do FSx console da Amazon, a Amazon cria FSx automaticamente um sistema de arquivos com uma única máquina virtual de armazenamento (SVM) e um volume, permitindo acesso rápido aos dados de instâncias Linux pelo protocolo Network File System (NFS). Ao criar o sistema de arquivos, você pode unir a SVM a um Active Directory para permitir o acesso de clientes Windows e macOS por meio do protocolo Server Message Block (SMB). Depois que seu sistema de arquivos for criado, você poderá criar volumes adicionais SVMs e conforme necessário.

Criar um sistema de arquivos (console)

Esse procedimento usa a opção de criação padrão para criar um sistema de arquivos FSx para ONTAP com uma configuração que você personaliza de acordo com suas necessidades. Para obter informações sobre como usar a opção de criação rápida para criar rapidamente um sistema de arquivos com um conjunto padrão de parâmetros de configuração, consulte Crie um sistema de arquivos Amazon FSx for NetApp ONTAP.

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel, escolha Criar sistema de arquivos.
3. Na página Selecionar tipo de sistema de arquivos, em Opções do sistema de arquivos, escolha Amazon FSx para NetApp ONTAP e, em seguida, escolha Avançar.
4. Na seção Método de criação, escolha Criação padrão.
5. Forneça as seguintes informações na seção Detalhes do sistema de arquivos:

   - Em Nome do sistema de arquivos (opcional), insira um nome para seu sistema de arquivos. É mais fácil encontrar e gerenciar seus sistemas de arquivos quando você define um nome para eles. É possível usar até 256 letras do Unicode, espaço em branco e números, além dos caracteres especiais + - = . _ : /
   - Em Tipo de implantação, escolha Multi-AZ 2, Single-AZ 2, Multi-AZ 1 ou Single-AZ 1.
     - Os sistemas de arquivos Multi-AZ replicam dados e oferecem suporte ao failover em várias zonas de disponibilidade dentro da mesma Região da AWS. O Multi-AZ 1 é a primeira geração do sistema FSx de arquivos ONTAP. A Multi-AZ 2 é um sistema de arquivos de segunda geração. Ambos são compatíveis com um par de alta disponibilidade (HA).
     - Os sistemas de arquivos single-AZ replicam os dados e oferecem failover automático em uma única zona de disponibilidade. O Single-AZ 1 é um sistema de arquivos ONTAP de

primeira geração FSx que suporta um par HA. A Single-AZ 2 é um sistema de arquivos do FSx para ONTAP de segunda geração compatível com até 12 pares de HA. Para obter mais informações, consulte Gerenciar pares de alta disponibilidade (HA).

Para obter mais informações sobre os tipos de implantação, consulte Opções de disponibilidade, durabilidade e implantação.

> **Note**
>
> Você não pode alterar o tipo de implantação do sistema de arquivos após a criação. Se quiser alterar o tipo de implantação (por exemplo, passar da Single-AZ 1 para a Single-AZ 2), você poderá fazer backup dos dados e restaurá-los em um novo sistema de arquivos. Você também pode migrar seus dados com NetApp SnapMirror AWS DataSync, com ou com uma ferramenta de cópia de dados de terceiros. Para obter mais informações, consulte Migrando FSx para o ONTAP usando NetApp SnapMirror e Migrando FSx para o ONTAP usando AWS DataSync.

- Em Capacidade de armazenamento SSD, informe a capacidade de armazenamento do sistema de arquivos, em gibibytes (GiB). Digite qualquer número inteiro no intervalo de 1.024 a 1.048.576 GiB (até 1 pebibyte [PiB]).

  Você pode aumentar a capacidade de armazenamento, conforme necessário, a qualquer momento após a criação do sistema de arquivos. Para obter mais informações, consulte Como gerenciar a capacidade de armazenamento.

- Em IOPS de SSD provisionadas, você tem duas opções para provisionar o número de IOPS para seu sistema de arquivos:
  - Escolha Automático (o padrão) se quiser que FSx a Amazon provisione automaticamente 3 IOPS por GiB de armazenamento SSD.
  - Escolha Provisionado pelo usuário se quiser especificar o número de IOPS. Você pode provisionar no máximo 200.000 IOPS de SSD por sistema de arquivos.

> **Note**
>
> Você pode aumentar suas IOPS de SSD provisionadas depois de criar o sistema de arquivos. Lembre-se de que o nível máximo de IOPS de SSD que o sistema de arquivos pode alcançar também é determinado pela capacidade de throughput do sistema de arquivos, mesmo ao provisionar IOPS de SSD adicionais. Para obter mais

informações, consulte Impacto da capacidade de throughput na performance e Como gerenciar a capacidade de armazenamento.

- Para a capacidade de taxa de transferência, você tem duas opções para determinar sua capacidade de taxa de transferência em megabytes por segundo (): MBps
  - Escolha Capacidade de transferência recomendada se quiser que FSx a Amazon escolha automaticamente a capacidade de transferência com base na quantidade de capacidade de armazenamento que você escolheu.
  - Escolha Especificar capacidade de throughput se quiser especificar a quantidade da capacidade de throughput. Se você escolher essa opção, uma lista suspensa Capacidade de throughput será exibida e preenchida com base no tipo de implantação que você escolheu. Você também poderá escolher o número de pares de HA (até 12). Para obter mais informações, consulte Gerenciar pares de alta disponibilidade (HA).

  Capacidade de throughput: é a velocidade sustentada na qual o servidor de arquivos que hospeda o sistema de arquivos pode fornecer dados. Para obter mais informações, consulte Amazon FSx para desempenho do NetApp ONTAP.

6. Na seção Redes, forneça as seguintes informações:

- Em Nuvem privada virtual (VPC), escolha a VPC que você deseja associar ao sistema de arquivos.
- Em Grupos de segurança da VPC, é possível escolher um grupo de segurança para associar à interface de rede do seu sistema de arquivos. Se você não especificar um, a Amazon FSx associará o grupo de segurança padrão da VPC ao seu sistema de arquivos.
- Especifique uma sub-rede para seu servidor de arquivos. Se você estiver criando um sistema de arquivos com várias AZs, escolha também uma Sub-rede em espera para o servidor de arquivos em espera.
- (Somente Multi-AZ) Para Tabelas de rotas da VPC, especifique as tabelas de rotas da VPC para criar endpoints do sistema de arquivos. Selecione todas as tabelas de rotas da VPC associadas às sub-redes nas quais seus clientes estão localizados. Por padrão, a Amazon FSx seleciona a tabela de rotas padrão da sua VPC. Para obter mais informações, consulte Acesso a dados de fora da VPC de implantação.

> **Note**
>
> A Amazon FSx gerencia essas tabelas de rotas para sistemas de arquivos Multi-AZ usando autenticação baseada em tags. Essas tabelas de rotas serão marcadas com `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Ao criar sistemas FSx de arquivos ONTAP Multi-AZ usando, AWS CloudFormation recomendamos que você adicione a `Key: AmazonFSx; Value: ManagedByAmazonFSx` tag manualmente.

- (Somente Multi-AZ) Intervalo de endereços IP do endpoint especifica o intervalo de endereços IP no qual são criados os endpoints para acessar o sistema de arquivos.

  Você tem três opções para o intervalo de endereços IP do endpoint:

  - Intervalo de endereços IP não alocados da sua VPC — A FSx Amazon escolhe os últimos 64 endereços IP do intervalo CIDR principal da VPC para usar como intervalo de endereços IP do endpoint para o sistema de arquivos. Esse intervalo será compartilhado entre vários sistemas de arquivos se você escolher essa opção várias vezes.

    > **Note**
    >
    > Essa opção ficará desabilitada se algum dos últimos 64 endereços IP no intervalo CIDR primário de uma VPC estiver sendo usado por uma sub-rede. Nesse caso, você ainda pode escolher um intervalo de endereços na VPC (ou seja, um intervalo que não esteja no final do intervalo CIDR primário ou um intervalo que esteja em um CIDR secundário da VPC) escolhendo a opção Inserir um intervalo de endereços IP.

  - Em Sub-rede preferencial, especifique uma Sub-rede para seu servidor de arquivos. Se você estiver criando um sistema de arquivos com várias AZs, escolha também uma Sub-rede em espera para o servidor de arquivos em espera.
  - (Somente Multi-AZ) Para Tabelas de rotas da VPC, especifique as tabelas de rotas da VPC para criar endpoints do sistema de arquivos. Selecione todas as tabelas de rotas da VPC associadas às sub-redes nas quais seus clientes estão localizados. Por padrão, a Amazon FSx seleciona a tabela de rotas padrão da sua VPC.
  - (Somente Multi-AZ) Intervalo de endereços IP do endpoint especifica o intervalo de endereços IP no qual são criados os endpoints para acessar o sistema de arquivos.

    Você tem três opções para o intervalo de endereços IP do endpoint:

- Intervalo de endereços IP não alocados da sua VPC — A FSx Amazon escolhe os últimos 64 endereços IP do intervalo CIDR principal da VPC para usar como intervalo de endereços IP do endpoint para o sistema de arquivos. Esse intervalo será compartilhado entre vários sistemas de arquivos se você escolher essa opção várias vezes.

  > **Note**
  >
  > Essa opção ficará desabilitada se algum dos últimos 64 endereços IP no intervalo CIDR primário de uma VPC estiver sendo usado por uma sub-rede. Nesse caso, você ainda pode escolher um intervalo de endereços na VPC (ou seja, um intervalo que não esteja no final do intervalo CIDR primário ou um intervalo que esteja em um CIDR secundário da VPC) escolhendo a opção Inserir um intervalo de endereços IP.

- Intervalo de endereços IP flutuante fora da sua VPC — A Amazon FSx escolhe um intervalo de endereços 198,1,x.0/24 que ainda não é usado por nenhum outro sistema de arquivos com a mesma VPC e tabelas de rotas.
- Inserir um intervalo de endereços IP: você pode fornecer um intervalo CIDR de sua escolha. O intervalo de endereços IP que você escolher poderá estar dentro ou fora do intervalo de endereços IP da VPC, desde que não se sobreponha a nenhuma sub-rede.

  > **Note**
  >
  > Não escolha nenhum intervalo que esteja dentro dos seguintes intervalos de CIDR, pois eles são incompatíveis com FSx o ONTAP:
  >
  > - 0.0.0.0/8
  > - 127.0.0.0/8
  > - 198.19.0.0/20
  > - 224.0.0.0/4
  > - 240.0.0.0/4
  > - 255.255.255.255/32

7. Na seção Criptografia, em Chave de criptografia, escolha a chave de criptografia AWS Key Management Service (AWS KMS) que protege os dados em repouso do seu sistema de arquivos.

8. Em Senha administrativa do sistema de arquivos, insira uma senha segura para o usuário `fsxadmin`. Confirme a senha.

   É possível utilizar o usuário `fsxadmin` para administrar o sistema de arquivos usando a CLI e a API REST do ONTAP. Para obter mais informações sobre o usuário `fsxadmin`, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

9. Na seção Configuração de máquina virtual de armazenamento padrão, forneça as seguintes informações:

   - No campo Nome da máquina virtual de armazenamento, forneça um nome para a máquina virtual de armazenamento. Você pode usar, no máximo, 47 caracteres alfanuméricos, além do caractere especial de sublinhado (_).
   - Para Senha administrativa da SVM, você pode escolher Especificar uma senha e fornecer uma senha para o usuário `vsadmin` da SVM. Você pode usar o usuário `vsadmin` para administrar a SVM utilizando a CLI ou a API REST do ONTAP. Para obter mais informações sobre o usuário `vsadmin`, consulte Gerenciando SVMs com o ONTAP CLI.

     Se você escolher Não especificar uma senha (o padrão), ainda poderá utilizar o usuário `fsxadmin` do sistema de arquivos para gerenciar o sistema usando a CLI ou a API REST do ONTAP, mas não poderá utilizar o usuário `vsadmin` da SVM para fazer o mesmo.
   - Para o estilo de segurança de volume, escolha entre Unix (Linux) e NTFS para o volume. Para obter mais informações, consulte Estilo de segurança do volume.
   - Na seção Active Directory, você pode unir um Active Directory à SVM. Para obter mais informações, consulte Trabalhando com o Microsoft Active Directory no FSx ONTAP.

     Se você não quiser unir a SVM a um Active Directory, escolha Não ingressar em um Active Directory.

     Se você quiser unir a SVM a um domínio autogerenciado do Active Directory, escolha Ingressar em um Active Directory e forneça os seguintes detalhes do Active Directory:

     - O nome NetBIOS do objeto de computador do Active Directory que será criado para a SVM. O nome NetBIOS não pode ter mais de 15 caracteres.
     - O nome totalmente qualificado do domínio do Active Directory. O nome do domínio não pode ter mais de 255 caracteres.
     - Endereços IP do servidor DNS — Os IPv4 endereços dos servidores do Sistema de Nomes de Domínio (DNS) do seu domínio.

- Nome de usuário da conta de serviço: o nome de usuário da conta de serviço no seu Active Directory existente. Não inclua um prefixo ou sufixo de domínio.
- Senha da conta de serviço: a senha da conta de serviço.
- Confirmar senha: a senha da conta de serviço.
- (Opcional) Unidade organizacional (UO): o nome do caminho distinto da unidade organizacional à qual você deseja unir seu sistema de arquivos.
- Grupo de administradores delegado do sistema de arquivos: o nome do grupo no Active Directory que pode administrar o sistema de arquivos.

  Se você estiver usando AWS Managed Microsoft AD, precisará especificar um grupo como Administradores AWS Delegados, FSx Administradores AWS Delegados ou um grupo personalizado com permissões delegadas à OU.

  Se você estiver ingressando em um AD autogerenciado, use o nome do grupo em seu AD. O grupo padrão é `Domain Admins`.

10. Na seção Configuração de volume padrão, você pode fornecer as seguintes informações para o volume padrão que é criado com seu sistema de arquivos:

    - No campo Nome do volume, forneça um nome para o volume. Você pode usar até 203 caracteres alfanuméricos ou sublinhado (_).
    - (Sistemas de arquivos com apenas um par de HA) Para o estilo de volume, escolha um FlexVol ou FlexGroup. FlexVol volumes são volumes de uso geral que podem ter até 300 tebibytes (TiB) de tamanho. FlexGroup os volumes são destinados a cargas de trabalho de alto desempenho e podem ter até 20 PiB de tamanho.
    - Em Tamanho do volume, insira qualquer número inteiro no intervalo de 20—314.572.800 mebibytes (MiB) para FlexVol volumes ou 800 gibibytes (GiB) — 2.400 TiB por par de HA para FlexGroup volumes. Por exemplo, um sistema de arquivos com 12 pares de HA teria um tamanho mínimo de volume de 9.600 GiB e um tamanho máximo de 20.480 TiB.
    - Para Tipo de volume, escolha Leitura-Gravação (RW) para criar um volume que seja legível e gravável ou Proteção de Dados (DP) para criar um volume que seja somente para leitura e possa ser usado como destino de um NetApp SnapMirror or SnapVault relacionamento. Para obter mais informações, consulte Tipos de volume.
    - Em Caminho da junção, insira um local no sistema de arquivos para montar o volume. O nome deve ter uma barra inicial, por exemplo `/vol3`.

- Para Eficiência de armazenamento, escolha Habilitado para habilitar os recursos de eficiência de armazenamento do ONTAP (eliminação da duplicação, compressão e compactação). Para obter mais informações, consulte Eficiência de armazenamento.
- Em Política de snapshots, escolha uma política de snapshots para o volume. Para obter mais informações sobre políticas de snapshots, consulte Políticas de snapshots.

  Se você escolher Política personalizada, especifique o nome da política no campo política personalizada. A política personalizada já deve existir na SVM ou no sistema de arquivos. Você pode criar uma política de snapshots personalizada com a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política de snapshot no NetApp Documentação do produto ONTAP.

11. Na seção Camadas padrão de armazenamento de volume, para Política de camadas do grupo de capacidade, escolha a política de camadas do grupo de armazenamento, que pode ser Automático (o padrão), Somente snapshot, Todos ou Nenhum. Para obter mais informações sobre políticas de camadas do grupo de capacidade, consulte Políticas de camadas de volume.

    Em Período de resfriamento da política de camadas, se você tiver definido camadas de armazenamento como `Auto` e `Snapshot-only`, os valores válidos das políticas serão de 2 a 183 dias. O período de resfriamento da política de camadas de um volume define o número de dias antes que os dados que não foram acessados sejam marcados como frios e movidos para o armazenamento do grupo de capacidade.

12. Na seção SnapLock Configuração de volume padrão, para SnapLock Configuração, escolha entre Ativado e Desativado. Para obter mais informações sobre como configurar um SnapLock Volume de conformidade ou um SnapLock Volume corporativo, consulte Noções básicas SnapLock Compliance Noções básicas SnapLock Enterprise e. Para obter mais informações sobre SnapLock, consulte Protegendo seus dados com SnapLock.

13. Em Backup e manutenção: opcional, você pode definir as seguintes opções:

    - Em Backup automático diário, escolha Habilitado para backups diários automáticos. Essa opção é habilitada por padrão.
    - Em Janela de backup automático diário, defina a hora do dia no Tempo Universal Coordenado (UTC) em que você deseja que a janela de backup automático diário seja iniciada. A janela é de 30 minutos a partir desse horário especificado. Essa janela não pode se sobrepor à janela de backup de manutenção semanal.
    - Para Período de retenção de backup automático, defina um período de 1 a 90 dias em que você deseja manter os backups automáticos.

- Para Janela de manutenção semanal, você pode definir a hora da semana em que deseja iniciar a janela de manutenção. O dia 1 é segunda-feira, o dia 2 é terça-feira, e assim por diante. A janela é de 30 minutos a partir desse horário especificado. Essa janela não pode se sobrepor à janela de backup automático diário.

14. Em Tags: opcional, você pode inserir uma chave e um valor para adicionar tags ao sistema de arquivos. Uma tag é um par de chave/valor que diferencia maiúsculas de minúsculas e ajuda você a gerenciar, filtrar e pesquisar o sistema de arquivos.

    Escolha Próximo.

15. Verifique a configuração do sistema de arquivos mostrada na página Criar sistema de arquivos. Para sua referência, anote quais configurações do sistema de arquivos você pode modificar após a criação do sistema de arquivos.
16. Escolha Create file system (Criar sistema de arquivos).

Criar um sistema de arquivos (CLI)

- Para criar um sistema de arquivos FSx for ONTAP, use o comando create-file-systemCLI (ou a operação de API CreateFileSystemequivalente), conforme mostrado no exemplo a seguir.

> **Note**
>
> Você não pode alterar o tipo de implantação do sistema de arquivos após a criação. Se quiser alterar o tipo de implantação (por exemplo, passar da Single-AZ 1 para a Single-AZ 2), você poderá fazer backup dos dados e restaurá-los em um novo sistema de arquivos. Você também pode migrar seus dados com NetApp SnapMirror AWS DataSync, com ou com uma ferramenta de cópia de dados de terceiros. Para obter mais informações, consulte Migrando FSx para o ONTAP usando NetApp SnapMirror e Migrando FSx para o ONTAP usando AWS DataSync.

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \

    --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
```

```
    --ontap-configuration DeploymentType=MULTI_AZ_1,
        ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

Depois de criar o sistema de arquivos com sucesso, a Amazon FSx retorna a descrição do sistema de arquivos no formato JSON, conforme mostrado no exemplo a seguir.


```
{
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
                "Mode": "AUTOMATIC",
                "Iops": 3072
      },
      "PreferredSubnetId": "subnet-abcdef1234567890b",
      "RouteTableIds": [
```

```
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
      ],
      "ThroughputCapacity": 512,
      "WeeklyMaintenanceStartTime": "4:10:00"
    }
  }
}
```

> **Note**
>
> Ao contrário do processo de criação de um sistema de arquivos no console, o comando `create-file-system` da CLI e a operação `CreateFileSystem` da API não criam uma SVM ou volume padrão. Para criar uma SVM, consulte Criar máquinas virtuais de armazenamento (SVM); para criar um volume, consulte Como criar volumes.

Criação FSx para sistemas de arquivos ONTAP em sub-redes compartilhadas

O compartilhamento de VPC permite que vários Contas da AWS criem recursos em nuvens privadas virtuais compartilhadas e gerenciadas centralmente (). VPCs Nesse modelo, a conta proprietária da VPC (proprietário) compartilha uma ou mais sub-redes com outras contas (participantes) que pertencem à mesma organização da. AWS Organizations

As contas de participantes podem ser criadas FSx para sistemas de arquivos ONTAP Single-AZ e Multi-AZ em uma sub-rede VPC que a conta do proprietário compartilhou com elas. Para que uma conta de participante crie um sistema de arquivos Multi-AZ, a conta do proprietário também precisa conceder FSx permissão à Amazon para modificar as tabelas de rotas nas sub-redes compartilhadas em nome da conta do participante. Para obter mais informações, consulte Como gerenciar a compatibilidade com VPC compartilhada para sistemas de arquivos Multi-AZ.

> **Note**
>
> A conta do participante é responsável pela coordenação com o proprietário da VPC para evitar a criação de qualquer sub-rede VPC subsequente que se sobreponha ao CIDR na VPC dos sistemas de arquivos do participante. Se houver sobreposição das sub-redes, o tráfego para o sistema de arquivos poderá ser interrompido.

Requisitos e considerações de sub-redes

Ao criar sistemas FSx de arquivos ONTAP em sub-redes compartilhadas, observe o seguinte:

- O proprietário da sub-rede VPC deve compartilhar uma sub-rede com uma conta participante antes que essa conta possa criar um sistema de arquivos FSx for ONTAP nela.
- Você não pode iniciar recursos usando o grupo de segurança padrão da VPC, pois ele pertence ao proprietário. Além disso, contas de participantes não podem iniciar recursos usando grupos de segurança que pertençam a outros participantes ou ao proprietário.
- Em uma sub-rede compartilhada, o participante e o proprietário controlam separadamente os grupos de segurança na respectiva conta. A conta proprietária poderá visualizar esses grupos de segurança criados pelos participantes, mas não poderá realizar nenhuma ação neles. Se a conta proprietário quiser remover ou modificar esses grupos de segurança, o participante que criou o grupo de segurança deverá executar a ação.
- As contas participantes podem exibir, criar, modificar e criar sistemas de arquivos Single-AZ e os recursos associados nas sub-redes que a conta do proprietário compartilhou com elas.
- As contas participantes podem criar, exibir, modificar e criar sistemas de arquivos Multi-AZ e os recursos associados nas sub-redes que a conta do proprietário compartilhou com elas. Além disso, a conta do proprietário também deve conceder permissões ao FSx serviço da Amazon para modificar as tabelas de rotas nas sub-redes compartilhadas em nome da conta do participante. Para obter mais informações, consulte Como gerenciar a compatibilidade com VPC compartilhada para sistemas de arquivos Multi-AZ.
- O proprietário da VPC compartilhada não poderá exibir, atualizar ou excluir recursos criados por um participante na sub-rede compartilhada. Isso é além dos recursos da VPC aos quais cada conta tem acesso diferente. Para obter mais informações, consulte Responsabilidades e permissões para proprietários e participantes no Guia do usuário do Amazon VPC.

Para obter informações, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

Ao compartilhar uma sub-rede de VPC

Ao compartilhar suas sub-redes com contas de participantes que serão criadas FSx para sistemas de arquivos ONTAP nas sub-redes compartilhadas, você precisará fazer o seguinte:

- O proprietário da VPC precisa usar AWS Resource Access Manager para compartilhar VPCs e sub-redes com segurança com outras pessoas. Contas da AWS Para obter mais informações, consulte Compartilhando seus AWS recursos no Guia AWS Resource Access Manager do usuário.
- O proprietário da VPC precisa compartilhar uma ou mais contas VPCs com uma conta de participante. Para obter mais informações, consulte Compartilhar as sub-redes da sua VPC com outras contas no Guia do usuário do Amazon Virtual Private Cloud.
- Para criar contas de participantes FSx para sistemas de arquivos ONTAP Multi-AZ, o proprietário da VPC também deve conceder ao FSx serviço da Amazon permissões para criar e modificar tabelas de rotas nas sub-redes compartilhadas em nome das contas dos participantes. Isso ocorre porque os sistemas de arquivos ONTAP Multi-AZ usam endereços IP flutuantes FSx para que os clientes conectados possam fazer a transição perfeita entre os servidores de arquivos preferenciais e os de espera durante um evento de failover. Quando ocorre um evento de failover, a Amazon FSx atualiza todas as rotas em todas as tabelas de rotas associadas ao sistema de arquivos para apontar para o servidor de arquivos atualmente ativo.

Como gerenciar a compatibilidade com VPC compartilhada para sistemas de arquivos Multi-AZ

As contas do proprietário podem gerenciar se as contas dos participantes podem ou não criar sistemas de arquivos Multi-AZ FSx para ONTAP em sub-redes VPC que o proprietário compartilhou com os participantes usando a API,, e AWS Management Console AWS CLI, conforme descrito nas seções a seguir.

Para gerenciar o compartilhamento de VPC para sistemas de arquivos Multi-AZ (console)

Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.

1. No painel de navegação, selecione Configurações.
2. Localize as Configurações de VPC compartilhada Multi-AZ na página Configurações.
    - Para habilitar o compartilhamento de VPC para sistemas de arquivos Multi-AZ em sub-redes da VPC que você compartilha, escolha Habilitar atualizações da tabela de rotas das contas participantes.
    - Para desativar o compartilhamento de VPC para sistemas de arquivos Multi-AZ em tudo o VPCs que você possui, escolha Desativar atualizações da tabela de rotas das contas dos participantes. A tela de confirmação será exibida.

> **Important**
>
> É altamente recomendável que os sistemas de arquivos Multi-AZ criados por participantes na VPC compartilhada sejam excluídos antes de você desabilitar esse recurso. Após a desabilitação do recurso, esses sistemas de arquivos entrarão em um estado `MISCONFIGURED` e correrão o risco de ficarem indisponíveis.

3. Insira **`confirm`** e escolha Confirmar para desabilitar o recurso.

Para gerenciar o compartilhamento de VPC para sistemas de arquivos Multi-AZ (AWS CLI)

1. Para visualizar a configuração atual do compartilhamento de VPC Multi-AZ, use o comando describe-shared-vpc-configurationCLI ou o comando de API DescribeSharedVpcConfigurationequivalente, mostrado a seguir:

   ```
   $ aws fsx describe-shared-vpc-configuration
   ```

   O serviço responde a uma solicitação bem-sucedida da seguinte forma:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
   }
   ```

2. Para gerenciar a configuração da VPC compartilhada Multi-AZ, use o comando update-shared-vpc-configurationCLI ou o comando equivalente da API. UpdateSharedVpcConfiguration O exemplo a seguir habilita o compartilhamento de VPC para sistemas de arquivos Multi-AZ.

   ```
   $ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
   ```

   O serviço responde a uma solicitação bem-sucedida da seguinte forma:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
   }
   ```

3. Para desabilitar o recurso, defina `EnableFsxRouteTableUpdatesFromParticipantAccounts` como `false`, conforme exibido no exemplo a seguir.

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-
participant-accounts false
```

O serviço responde a uma solicitação bem-sucedida da seguinte forma:

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

Atualizar sistemas de arquivos

Este tópico explica quais propriedades de um sistema de arquivos existente você pode atualizar e fornece procedimentos para fazer isso usando o FSx console e a CLI da Amazon. Você pode atualizar o seguinte FSx para as propriedades do sistema de arquivos ONTAP usando o FSx console e a API da Amazon: AWS CLI

- Backups automáticos diários. Ativa ou desativa os backups automáticos diários, modifica a janela de backup e o período de retenção do backup. Para obter mais informações, consulte Backups automáticos diários.
- Janela de manutenção semanal. Define o dia da semana e a hora em que FSx a Amazon realiza a manutenção e as atualizações do sistema de arquivos. Para obter mais informações, consulte Otimizando o desempenho com as janelas de FSx manutenção da Amazon.
- Senha administrativa do sistema de arquivos. Altera a senha do usuário `fsxadmin` do sistema de arquivos. É possível utilizar o usuário `fsxadmin` para administrar o sistema de arquivos usando a CLI e a API REST do ONTAP. Para obter mais informações sobre o usuário `fsxadmin`, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.
- Tabelas de rotas da Amazon VPC. Com os sistemas de arquivos Multi-AZ FSx para ONTAP, os endpoints que você usa para acessar dados via NFS ou SMB e os endpoints de gerenciamento para acessar a CLI, a API e o BlueXP do ONTAP usam endereços IP flutuantes nas tabelas de rotas da Amazon VPC que você associa ao seu sistema de arquivos. Você pode associar novas tabelas de rotas que você cria aos seus sistemas de arquivos com várias AZs existentes, permitindo que você configure quais clientes podem acessar seus dados mesmo à medida que

sua rede evolui. Você também pode desassociar (remover) as tabelas de rotas existentes do seu sistema de arquivos.

> **Note**
>
> A Amazon FSx gerencia tabelas de rotas de VPC para sistemas de arquivos Multi-AZ usando autenticação baseada em tags. Essas tabelas de rotas serão marcadas com `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Ao criar ou atualizar FSx para sistemas de arquivos ONTAP Multi-AZ usando, AWS CloudFormation recomendamos que você adicione a `Key: AmazonFSx; Value: ManagedByAmazonFSx` tag manualmente.

Atualizar um sistema de arquivos (console)

Os procedimentos a seguir fornecem instruções sobre como fazer atualizações em um sistema de arquivos existente FSx do ONTAP usando o. AWS Management Console

Atualizar backups automáticos diários

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Para exibir a página de detalhes do sistema de arquivos, no painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema FSx de arquivos ONTAP que você deseja atualizar.
3. Escolha a guia Backups no segundo painel da página.
4. Selecione Atualizar.
5. Modifique as configurações de backup automático diário desse sistema de arquivos.
6. Escolha Salvar para salvar as alterações.

Atualizar a janela de manutenção semanal

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Para exibir a página de detalhes do sistema de arquivos, no painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema FSx de arquivos ONTAP que você deseja atualizar.
3. Escolha a guia Administração no segundo painel da página.
4. No painel Manutenção, escolha Atualizar.

5. Modifique quando a janela de manutenção semanal ocorre para esse sistema de arquivos.
6. Escolha Salvar para salvar as alterações.

Alterar a senha administrativa do sistema de arquivos

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Para exibir a página de detalhes do sistema de arquivos, no painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema FSx de arquivos ONTAP que você deseja atualizar.
3. Escolha a guia Administração.
4. No painel Administração do ONTAP, escolha Atualizar em Senha do administrador ONTAP.
5. Na caixa de diálogo Atualizar credenciais de administrador ONTAP, digite uma nova senha no campo Senha administrativa do ONTAP.
6. Use o campo Confirmar senha para confirmar a senha.
7. Escolha Atualizar credenciais para salvar sua alteração.

> **Note**
>
> Se você receber um erro informando que a nova senha não atende aos requisitos de senha, você pode usar o `security login role config show` ONTAP Comando CLI para visualizar as configurações de requisitos de senha no sistema de arquivos. Para obter mais informações, incluindo instruções sobre como alterar a configuração de senha, consulte Falha na atualização da senha da conta `fsxadmin`.

Para atualizar tabelas de rotas de VPC em sistemas de arquivos Multi-AZ

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Para exibir a página de detalhes do sistema de arquivos, no painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema FSx de arquivos ONTAP que você deseja atualizar.
3. Em Ações, escolha Gerenciar tabelas de rotas. Essa opção só está disponível para sistemas de arquivos com várias AZs.
4. Na caixa de diálogo Gerenciar tabelas de rotas, faça o seguinte:

- Para associar uma nova tabela de rotas de VPC, selecione uma tabela de rotas na lista suspensa Associar novas tabelas de rotas e escolha Associar.
- Para desassociar uma tabela de rotas de VPC existente, selecione uma tabela de rotas no painel Tabelas de rotas atuais e escolha Desassociar.

5. Escolha Fechar.

Atualizar um sistema de arquivos (CLI)

O procedimento a seguir ilustra como fazer atualizações em um sistema de arquivos existente FSx para ONTAP usando o. AWS CLI

1. Para atualizar a configuração de um sistema de arquivos FSx for ONTAP, use o comando update-file-systemCLI (ou a operação de API UpdateFileSystemequivalente), conforme mostrado no exemplo a seguir.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
      FsxAdminPassword=new-fsx-admin-password
```

2. Para desabilitar backups diários automáticos, defina a propriedade `AutomaticBackupRetentionDays` como 0.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

Gerenciar pares de alta disponibilidade (HA)

Cada sistema FSx de arquivos do ONTAP é alimentado por um ou mais pares de servidores de arquivos de alta disponibilidade (HA) em uma configuração ativa em espera. Nessa configuração, há um servidor de arquivos preferencial que fornece tráfego ativamente e um servidor de arquivos secundário que assume o controle se o servidor ativo não estiver disponível. FSx para ONTAP, os sistemas de arquivos de primeira geração são alimentados por um par de HA, que oferece até 4% GBps da capacidade de taxa de transferência e 160.000 SSD. IOPs FSx para ONTAP, os sistemas

de arquivos Multi-AZ de segunda geração também são alimentados por um par de HA e oferecem até 6% GBps da capacidade de taxa de transferência e 200.000 SSD IOPS. FSx para ONTAP, os sistemas de arquivos Single-AZ de segunda geração são alimentados por até 12 pares de HA, que podem fornecer até 72 de capacidade de taxa GBps de transferência e 2.400.000 IOPS de SSD (6 de capacidade de taxa de transferência e 200.000 IOPS de SSD por par GBps de HA).

Quando você cria seu sistema de arquivos a partir do FSx console da Amazon, a Amazon FSx recomenda o número de pares de HA que você deve usar com base no armazenamento SSD desejado. Você também poderá escolher manualmente o número de pares de HA com base na workload e nos requisitos de desempenho. Recomendamos que você use um único par de HA se os requisitos do sistema de arquivos forem atendidos por até 6% GBps da capacidade de taxa de transferência e 200.000 SSDs IOPs, e vários pares de HA se suas cargas de trabalho precisarem de níveis mais altos de escalabilidade de desempenho.

Cada par de HA tem um agregado, que é um conjunto lógico de discos físicos.

> **Note**
>
> Você pode adicionar pares de HA aos sistemas de arquivos Single-AZ de segunda geração. Para obter mais informações, consulte Adicionar pares de alta disponibilidade (HA). Caso contrário, você pode migrar dados entre sistemas de arquivos (com diferentes pares de HA) usando SnapMirror, AWS DataSync, ou restaurando seus dados de um backup para um novo sistema de arquivos.

Adicionar pares de alta disponibilidade (HA)

FSx for ONTAP, os sistemas de arquivos são compostos por um ou mais pares HA de servidores de arquivos. Os sistemas de arquivos de primeira geração e os sistemas de arquivos Multi-AZ de segunda geração têm um par de HA, e os sistemas de arquivos Single-AZ de segunda geração têm até 12 pares de HA. Você também pode adicionar mais pares de HA depois de criar um sistema de arquivos Single-AZ de segunda geração (até um máximo de 12). Adicionar pares de HA não causa interrupções e a conclusão da operação normalmente leva apenas alguns minutos.

Considere os seguintes pontos ao adicionar pares de HA ao seu sistema de arquivos:

- Adicionar pares de HA ao seu sistema de arquivos introduz novos servidores de arquivos com armazenamento próprio (ou agregado). Os novos pares de HA têm a mesma capacidade de throughput e capacidade de armazenamento dos pares de HA existentes do seu sistema de

arquivos. Por exemplo, suponha que seu sistema de arquivos tenha dois pares de HA com um total de 12 de capacidade GBps de taxa de transferência e 2 tebibytes (TiB) de armazenamento SSD. Se você adicionar um novo par de HA, seu sistema de arquivos terá 18% GBps da capacidade de taxa de transferência e 3 TiB de armazenamento SSD.

- Para se beneficiar do desempenho adicional dos novos pares de HA, você precisará mover alguns de seus volumes existentes para os novos pares de HA e remontar os clientes para se conectarem a eles. Para obter mais informações, consulte Equilibrando cargas de trabalho entre pares de HA.
- Você não pode modificar a capacidade de throughput, a capacidade de armazenamento SSD ou as IOPS SSD provisionadas do seu sistema de arquivos ao adicionar pares de HA ou enquanto houver uma atualização para adicionar pares de HA em andamento.
- Você não pode remover pares de HA após adicioná-los. Recomendamos escalar a capacidade de throughput do sistema de arquivos se você precisar de mais desempenho temporariamente (supondo que o sistema de arquivos não tenha a maior capacidade de throughput). Isso aumenta a capacidade de throughput dos pares de HA existentes do seu sistema de arquivos.
- Para aumentar os pares de HA em um sistema de arquivos de segunda geração de um para dois ou mais pares, seu sistema de arquivos poderá ter no máximo cinco SVMS.
- O protocolo iSCSI está disponível em sistemas de arquivos que têm até seis pares de alta disponibilidade (pares de HA). O protocolo NVMe /TCP está disponível em sistemas de arquivos de segunda geração que têm seis ou menos pares de HA. Para obter mais informações, consulte Acessando seus dados FSx do ONTAP.
- Quando você adiciona novos pares de HA ao seu sistema de arquivos, o NVMe cache é ativado por padrão para os novos nós do sistema de arquivos. Recomendamos desabilitá-lo para workloads com alto throughput. Para obter mais informações, consulte Gerenciando o NVMe cache.

Para adicionar pares de HA

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Para exibir a página de detalhes do sistema de arquivos, no painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema FSx de arquivos ONTAP que você deseja atualizar.
3. No painel Resumo, em Número de pares de HA, escolha Atualizar.
4. No menu suspenso Pares de HA, selecione o número de pares de HA que você deseja adicionar ao sistema de arquivos.

5. Escolha o botão Atualizar.

Depois de adicionar pares de HA, é importante reequilibrar os dados existentes para garantir que a E/S permaneça distribuída uniformemente entre os pares de HA do sistema de arquivos. Para obter mais informações, consulte Equilibrando cargas de trabalho entre pares de HA.

Equilibrando cargas de trabalho entre pares de HA

Se você tem um sistema de arquivos com vários pares de alta disponibilidade (HA), sua taxa de transferência e armazenamento estão distribuídos por cada um dos pares de HA. FSx for ONTAP equilibra automaticamente seus arquivos à medida que eles são gravados em seu sistema de arquivos, mas seus dados de carga de trabalho e E/S não são mais balanceados quando você adiciona pares de HA. Além disso, em casos raros, os dados ou a E/S da workload podem ficar desequilibrados nos pares de HA existentes do sistema de arquivos, o que pode afetar o desempenho geral da workload. Se sua workload estiver desequilibrada, você poderá rebalanceá-la em cada um dos pares de HA do seu sistema de arquivos (e em seus respectivo servidores de arquivos e agregados proporcionais, os grupos de armazenamento que compõem seu nível de armazenamento primário).

Tópicos

- Balanceamento de utilização do armazenamento principal
- Desequilíbrio na utilização de desempenho do servidor de arquivos e do disco
- Mapeamento de CloudWatch dimensões para recursos da CLI do ONTAP e da API REST
- Rebalancear clientes
- Rebalancear volumes

Balanceamento de utilização do armazenamento principal

A capacidade de armazenamento principal do seu sistema de arquivos é dividida igualmente entre cada um dos seus pares de HA em grupos de armazenamento chamados de agregados. Cada par de HA tem um agregado. Recomendamos que você mantenha uma utilização média não superior a 80% para seu nível de armazenamento principal de forma contínua. Para sistemas de arquivos com vários pares de HA, recomendamos que você mantenha uma utilização média de até 80% para cada agregado.

Manter 80% de utilização garante que haja espaço livre para novos dados recebidos e mantém uma sobrecarga saudável para as operações de manutenção, que podem reivindicar temporariamente o espaço livre em seus agregados.

Se você perceber que seus agregados estão desequilibrados, é possível aumentar a capacidade de armazenamento principal do seu sistema de arquivos (aumentando proporcionalmente a capacidade de armazenamento de cada agregado) ou mover seus volumes entre agregados. Para obter mais informações, consulte Mover volumes entre agregados.

Desequilíbrio na utilização de desempenho do servidor de arquivos e do disco

Os recursos de desempenho total do seu sistema de arquivos (como throughput de rede, throughput e IOPS de servidor de arquivos para disco e IOPS de disco) são divididos igualmente entre os pares de HA do sistema de arquivos. Recomendamos que você mantenha uma utilização média abaixo de 50% (com um pico máximo de utilização abaixo de 80%) continuamente para todos os limites de desempenho; isso vale tanto para a utilização geral dos recursos do servidor de arquivos do seu sistema de arquivos em todos os pares de HA quanto para cada servidor de arquivos.

Se você perceber que a utilização do desempenho do servidor de arquivos está desequilibrada (e que os servidores de arquivos nos quais sua workload está desequilibrada têm uma utilização contínua superior a 80%), você poderá usar a CLI e a API REST do ONTAP para diagnosticar adicionalmente a causa do desequilíbrio de desempenho e corrigi-la. Veja a seguir uma tabela com possíveis indicadores de desequilíbrio e as próximas etapas para diagnósticos adicionais.

Se o respectivo elemento do seu sistema de arquivos…	Então...
O throughput de disco do servidor de arquivos ou as IOPS de disco do servidor de arquivos estiverem desequilibrados	Talvez você esteja enfrentando pontos de críticos de E/S em um subconjunto de pares de HA (um subconjunto de seus volumes com uma grande quantidade de dados sendo acessados), o que pode limitar o desempenho geral de sua workload porque está criando um gargalo em relação a um subconjunto de pares de HA. Para cada servidor de arquivos altamente utilizado, verifique os volumes mais utilizados para ver quais volumes têm mais atividade em um agregado. Para obter mais informações sobre esse procedimento, consulte Rebalancear volumes.
O throughput da rede estiver desequilibrado,	Seus dados estão distribuídos uniformemente entre os pares de HA, mas seus clientes não. Para os servidores de arquivos que têm mais

Se o respectivo elemento do seu sistema de arquivos…	Então...
mas o throughput de disco do servidor de arquivos, as IOPS de disco do servidor de arquivos ou as IOPS de disco não estiverem desequilibrados	utilização de throughput da rede do que outros, verifique os principais clientes de cada servidor de arquivos e, em seguida, reequilibre esses clientes desmontando todos os volumes desses clientes e remontando-os usando um endpoint diferente em um par de HA diferente. Para obter mais informações sobre esse procedimento, consulte Rebalancear clientes.

Mapeamento de CloudWatch dimensões para recursos da CLI do ONTAP e da API REST

Seu sistema de arquivos de segunda geração tem CloudWatch métricas da Amazon com a `Aggregate` dimensão `FileServer` or. Para diagnosticar adicionalmente os casos de desequilíbrio, você precisa mapear esses valores de dimensão para servidores de arquivos específicos (ou nós) e agregados na CLI ou na API REST do ONTAP.

- Para servidores de arquivos, cada nome de servidor de arquivos é mapeado para um nome de servidor de arquivos (ou nó) no ONTAP (por exemplo, `FsxId01234567890abcdef-01`). Os servidores de arquivos com números ímpares são servidores preferenciais de arquivos (ou seja, eles atendem ao tráfego, a menos que o sistema de arquivos tenha feito failover para o servidor de arquivos secundário), enquanto os servidores de arquivos com números pares são servidores secundários de arquivos (ou seja, eles só atendem ao tráfego quando o par não estiver disponível). Por esse motivo, os servidores secundários de arquivos normalmente mostrarão menos utilização do que os servidores preferenciais de arquivos.
- Para agregados, cada nome agregado é mapeado para um agregado no ONTAP (por exemplo, `aggr1`). Há um agregado para cada par de HA, o que significa que o agregado `aggr1` é compartilhado por servidores de arquivos `FsxId01234567890abcdef-01` (o servidor de arquivos ativo) e `FsxId01234567890abcdef-02` (o servidor de arquivos secundário) em um par de HA, o agregado `aggr2` é compartilhado por servidores de arquivos `FsxId01234567890abcdef-03` e `FsxId01234567890abcdef-04` e assim por diante.

Você pode visualizar os mapeamentos entre todos os agregados e servidores de arquivos usando a CLI do ONTAP.

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar o NetApp ONTAP CLI do usuário do Amazon FSx for NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Use o comando storage aggregate show, especificando o parâmetro `-fields node`.

   ```
   ::> storage aggregate show -fields node
   aggregate                     node
   ----------------------------- ------------------------
   aggr1                         FsxId01234567890abcdef-01
   aggr2                         FsxId01234567890abcdef-03
   aggr3                         FsxId01234567890abcdef-05
   aggr4                         FsxId01234567890abcdef-07
   aggr5                         FsxId01234567890abcdef-09
   aggr6                         FsxId01234567890abcdef-11
   6 entries were displayed.
   ```

Rebalancear clientes

Após adicionar pares de HA ou se você estiver enfrentando um desequilíbrio de E/S nos servidores de arquivos (especificamente com a utilização da throughput da rede), você poderá reequilibrar seus clientes. Se você estiver reequilibrando clientes após adicionar pares de HA, pule para Remontar clientes. Caso contrário, primeiro você deve identificar os clientes com tráfego elevado que você deseja mover para reequilibrar a E/S da workload.

Se estiver enfrentando um desequilíbrio de E/S nos servidores de arquivos (especificamente com a utilização da throughput da rede), clientes com E/S elevados podem ser a causa. Para identificar clientes com tráfego elevado, use a CLI do ONTAP.

Identificar clientes com tráfego elevado

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar o NetApp ONTAP CLI do usuário do Amazon FSx for NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Para visualizar os clientes com maior nível de tráfego, use o comando statistics top client show na CLI do ONTAP. Opcionalmente, você pode especificar o parâmetro `-node` para visualizar somente os principais clientes de um servidor de arquivos específico. Se você estiver diagnosticando um desequilíbrio em um servidor de arquivos específico, use o parâmetro `-node`, substituindo-o `node_name` pelo nome do servidor de arquivos (por exemplo, `FsxId01234567890abcdef-01`).

   Opcionalmente, você pode adicionar o parâmetro `-interval`, fornecendo o intervalo durante o qual fazer a medição (em segundos) antes da produção de cada relatório. Aumentar o intervalo (por exemplo, até o máximo de 300 segundos) fornecerá uma amostra de longo prazo da quantidade de tráfego direcionada para cada volume. O padrão é 5 (segundos).

   ```
   ::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
   ```

   Na saída, os principais clientes serão mostrados por endereço IP e pela porta.

   ```
                                                    *Total     Total
               Client   Vserver          Node           Ops     (Bps)
   ------------------- --------- ------------------------- ------ ---------
    172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
   172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
   ```

Remontar clientes

- Você pode reequilibrar clientes com outros pares de HA. Para fazer isso, desmonte o volume do cliente e remonte-o usando o nome de DNS do endpoint NFS/SMB da SVM. Isso retornará um endpoint aleatório correspondente a um par HA aleatório.

  Recomendamos que você reutilize o nome de DNS, mas você tem a opção de escolher explicitamente qual par de HA um determinado cliente montará. Para garantir que você esteja montando um cliente em um endpoint diferente, você pode especificar um endereço IP de endpoint diferente daquele que corresponde ao servidor de arquivos que está enfrentando tráfego elevado. Como alternativa, você pode fazer isso executando o seguinte comando :

```
::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
 address,curr-node
vserver   lif                  address      curr-node
--------- -------------------- ------------ ------------------------
svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
svm01 nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
2 entries were displayed.
```

De acordo com o exemplo de saída do comando `statistics top client show`, o cliente `172.17.236.53` está direcionando tráfego intenso para `FsxId01234567890abcdef-01`. A saída do comando `network interface show` indica que esse é o endereço `172.31.15.89`. Para montar em um endpoint diferente, selecione qualquer outro endereço (neste exemplo, o único outro endereço é `172.31.8.112`, correspondente a `FsxId01234567890abcdef-03`).

Rebalancear volumes

Se você estiver enfrentando um desequilíbrio de E/S em seus volumes ou agregados, é possível reequilibrar os volumes para redistribuir o tráfego de E/S entre seus volumes.

> **Note**
>
> Se estiver enfrentando um desequilíbrio na utilização do armazenamento em seus agregados, geralmente não há nenhum impacto sobre o desempenho, a menos que a alta utilização esteja associada ao desequilíbrio de E/S. Embora você possa mover volumes entre agregados para equilibrar a utilização do armazenamento, só recomendamos mover volumes se você estiver observando um impacto no desempenho, pois a movimentação de volumes pode ter um impacto adverso sobre o desempenho se você também não considerar a E/S direcionada para cada volume que você está pensando em mover.

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar o NetApp ONTAP CLI do usuário do Amazon FSx for NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Use o comando statistics volume show da CLI do ONTAP para visualizar os volumes com maior tráfego para um determinado agregado, com as seguintes alterações:

- *aggregate_name*Substitua pelo nome do agregado (por exemplo,`aggr1`).
- Opcionalmente, você pode adicionar o parâmetro `-interval`, fornecendo o intervalo durante o qual fazer a medição (em segundos) antes da produção de cada relatório. Aumentar o intervalo (por exemplo, até o máximo de 300 segundos) fornecerá uma amostra de longo prazo da quantidade de tráfego direcionada para cada volume. O padrão é 5 (segundos).

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
 [5,300]]
```

Dependendo do intervalo escolhido, a exibição dos dados poderá levar até 5 minutos. O comando mostra todos os volumes no agregado, junto com a quantidade de tráfego direcionada para cada agregado.

```
                          *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (us)
---------- ------- --------- ------ ---- ----- ----- --------- ----- -------
vol1__0007    svm1     aggr1   4078 4078     0     0 267255808     0    1092
vol1__0005    svm1     aggr1   4078 4078     0     0 267255808     0    1086
vol1__0003    svm1     aggr1   4077 4077     0     0 267223040     0    1086
vol1__0001    svm1     aggr1   4077 4077     0     0 267239424     0    1087
vol1__0008    svm1     aggr2   2314 2314     0     0 151650304     0    1112
vol1__0006    svm1     aggr2   2144 2144     0     0 140509184     0    1104
vol1__0002    svm1     aggr2   2183 2183     0     0 143065088     0    1106
vol1__0004    svm1     aggr2   2183 2183     0     0 143065088     0    1103
```

As estatísticas de volume são mostradas por constituinte (por exemplo, `vol1__0015` é o 15º constituinte de FlexGroup `vol1`). Você pode ver na saída do exemplo que os constituintes de `aggr1` são mais utilizados do que os constituintes de. `aggr2` Para equilibrar o tráfego entre agregados, você pode mover os volumes constituintes entre os agregados para que o tráfego seja distribuído de modo mais uniforme.

3. Se você tiver adicionado novos pares de HA, deverá mover os volumes existentes para novos agregados. Para obter mais informações, consulte Mover volumes entre agregados.

Gerenciando o NVMe cache

O NVMe cache é ativado por padrão em seu sistema de arquivos de segunda geração. Se seu sistema de arquivos de segunda geração tiver uma carga de trabalho com muita taxa de transferência, você poderá desativar o cache para melhorar o NVMe desempenho. O procedimento a seguir explica como ativar, desativar e validar o NVMe cache do sistema de arquivos.

Para gerenciar o NVMe cache

1. SSH em seu ONTAP sistema de arquivos. Para obter mais informações, consulte the section called “Usar o NetApp ONTAP CLI”.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Usar a system node external-cache modify ONTAP Comando CLI. Escolha **`true`** ativar ou desativar **`false`** o NVMe cache.

   ```
   ::> system node external-cache modify -node * -is-enabled [true|false]
   ```

3. Usar a system node external-cache show ONTAP Comando CLI para verificar se o NVMe cache está ativado ou desativado.

   ```
   ::> system node external-cache show -node * -fields is-enabled
   ```

O NVMe cache é ativado ou desativado por nó. Quando você adiciona novos pares de alta disponibilidade (HA) ao seu sistema de arquivos, cada novo nó tem o mesmo comportamento padrão dos nós de um novo sistema de arquivos. Portanto, o NVMe cache seria habilitado para qualquer novo nó em um sistema de arquivos, mesmo que os nós existentes o tivessem desativado. Para obter mais informações, consulte Adicionar pares de alta disponibilidade (HA).

Monitorar detalhes do sistema de arquivos

Você pode visualizar informações detalhadas de configuração do seu sistema FSx de arquivos do ONTAP usando o FSx console da Amazon AWS CLI, o e a API e é compatível AWS SDKs.

Para visualizar informações detalhadas do sistema de arquivos:

- Como usar o console: escolha um sistema de arquivos para visualizar a página de detalhes dos Sistemas de arquivos. O painel Resumo mostra o ID do sistema de arquivos, o status do ciclo de

vida, o tipo de implantação, a capacidade de armazenamento SSD, a capacidade de throughput, as IOPS provisionadas, as zonas de disponibilidade e o horário de criação.

As guias a seguir fornecem informações detalhadas de configuração e edição de propriedades que podem ser modificadas:

- Segurança e rede
- Monitoramento e desempenho — Exibe CloudWatch alarmes que você criou e métricas e avisos para as seguintes categorias:
  - Resumo: resumo de alto nível das métricas de atividade do sistema de arquivos
  - Capacidade de armazenamento do sistema de arquivos
  - Desempenho de disco e do servidor de arquivos

  Para obter mais informações, consulte Monitoramento com a Amazon CloudWatch.
- Administração: exibe as seguintes informações de administração do sistema de arquivos:
  - A ferramenta DNS nomes e IP endereços do gerenciamento do sistema de arquivos e dos endpoints entre clusters.
  - A ferramenta ONTAP nome de usuário do administrador.
  - A opção de atualizar o ONTAP senha do administrador.
- Lista do sistema de arquivos SVMs
- Lista dos volumes do sistema de arquivos
- Configurações de backup: altere a configuração de backup diário automático do sistema de arquivos.
- Atualizações: mostra o status das atualizações iniciadas pelo usuário feitas na configuração do sistema de arquivos.
- Tags: visualize, edite, adicione, remova pares de tags chave:valor.
- Usando a CLI ou a API — Use o comando da describe-file-systemsCLI ou a operação da API. DescribeFileSystems

FSx para o status do sistema de arquivos ONTAP

Você pode visualizar o status de um sistema de FSx arquivos da Amazon usando o FSx console da Amazon, o AWS CLI comando describe-file-systemsou a operação da API DescribeFileSystems.

Status do sistema de arquivos	Descrição
DISPONÍVEL	O sistema de arquivos foi criado com êxito e está disponível para uso.
CRIANDO	A Amazon FSx está criando um novo sistema de arquivos.
EXCLUINDO	A Amazon FSx está excluindo um sistema de arquivos existente.
CONFIGURAÇÃO INCORRETA	O sistema de arquivos está em um estado de configuração incorreta, mas recuperável.
COM FALHA	1. O sistema de arquivos falhou e a Amazon não FSx consegue recuperá-lo. 2. Ao criar um novo sistema de arquivos, a Amazon não FSx conseguiu criar um novo sistema de arquivos.

Excluir sistemas de arquivos

Você pode excluir um sistema FSx de arquivos do ONTAP usando o FSx console da Amazon AWS CLI, o e a FSx API da Amazon e. SDKs

Para excluir um sistema de arquivos:

- Como usar o console: siga o procedimento descrito em Limpar os recursos.
- Usando a CLI ou a API — primeiro exclua todos os volumes e SVMs em seu sistema de arquivos. Em seguida, use o comando da delete-file-systemCLI ou a operação da DeleteFileSystemAPI.

Gerenciamento FSx de máquinas virtuais de armazenamento ONTAP

No FSx ONTAP, os volumes são hospedados em servidores de arquivos virtuais chamados de máquinas virtuais de armazenamento (SVMs). Uma SVM é um servidor de arquivos isolado com

suas próprias credenciais administrativas e endpoints para administrar e acessar dados. Quando você acessa dados no FSx ONTAP, seus clientes e estações de trabalho montam um volume, compartilhamento SMB ou LUN iSCSI hospedado por uma SVM usando o endpoint (endereço IP) da SVM.

A Amazon cria FSx automaticamente uma SVM padrão em seu sistema de arquivos quando você cria um sistema de arquivos usando o. AWS Management Console Você pode criar mais SVMs em seu sistema de arquivos a qualquer momento usando o console ou a FSx API da Amazon SDKs e. AWS CLI Você não pode criar SVMs usando a CLI do ONTAP ou a API REST.

Você pode associá-lo SVMs a um Microsoft Active Directory para autenticação e autorização de acesso a arquivos. Para obter mais informações, consulte Trabalhando com o Microsoft Active Directory no FSx ONTAP.

Número máximo de SVMs por sistema de arquivos

A tabela a seguir lista o número máximo SVMs que você pode criar para um sistema de arquivos. O número máximo de SVMs depende da quantidade de capacidade de transferência provisionada em megabytes por segundo (). MBps

Pares de alta disponibilidade (HA)	Quantidade de capacidade de processamento () MBps	Número máximo de SVMs por sistema de arquivos
1 par de HA	128	6
	256	6
	384	6
	512	14
	768	14
	1,024	14
	1.536	14
	2.048	24
	3.072	14

Pares de alta disponibilidade (HA)	Quantidade de capacidade de processamento () MBps	Número máximo de SVMs por sistema de arquivos
	4.096	24
	6,144	24
2 a 12 pares de HA	Any	5

Tópicos

- Criar máquinas virtuais de armazenamento (SVM)
- Atualizar máquinas virtuais de armazenamento (SVM)
- Auditar acesso a arquivos
- Configurando um servidor SMB em um grupo de trabalho
- Detalhes de configuração da máquina virtual de armazenamento (SVM)
- Excluir máquinas virtuais de armazenamento (SVM)

Criar máquinas virtuais de armazenamento (SVM)

Você pode criar um FSx para o ONTAP SVM usando a AWS Management Console API AWS CLI, e.

O número máximo SVMs que você pode criar para um sistema de arquivos depende do tipo de implantação do sistema de arquivos e da quantidade de capacidade de transferência provisionada. Para obter mais informações, consulte Número máximo de SVMs por sistema de arquivos.

Propriedades da SVM

Ao criar uma SVM, defina as propriedades a seguir.

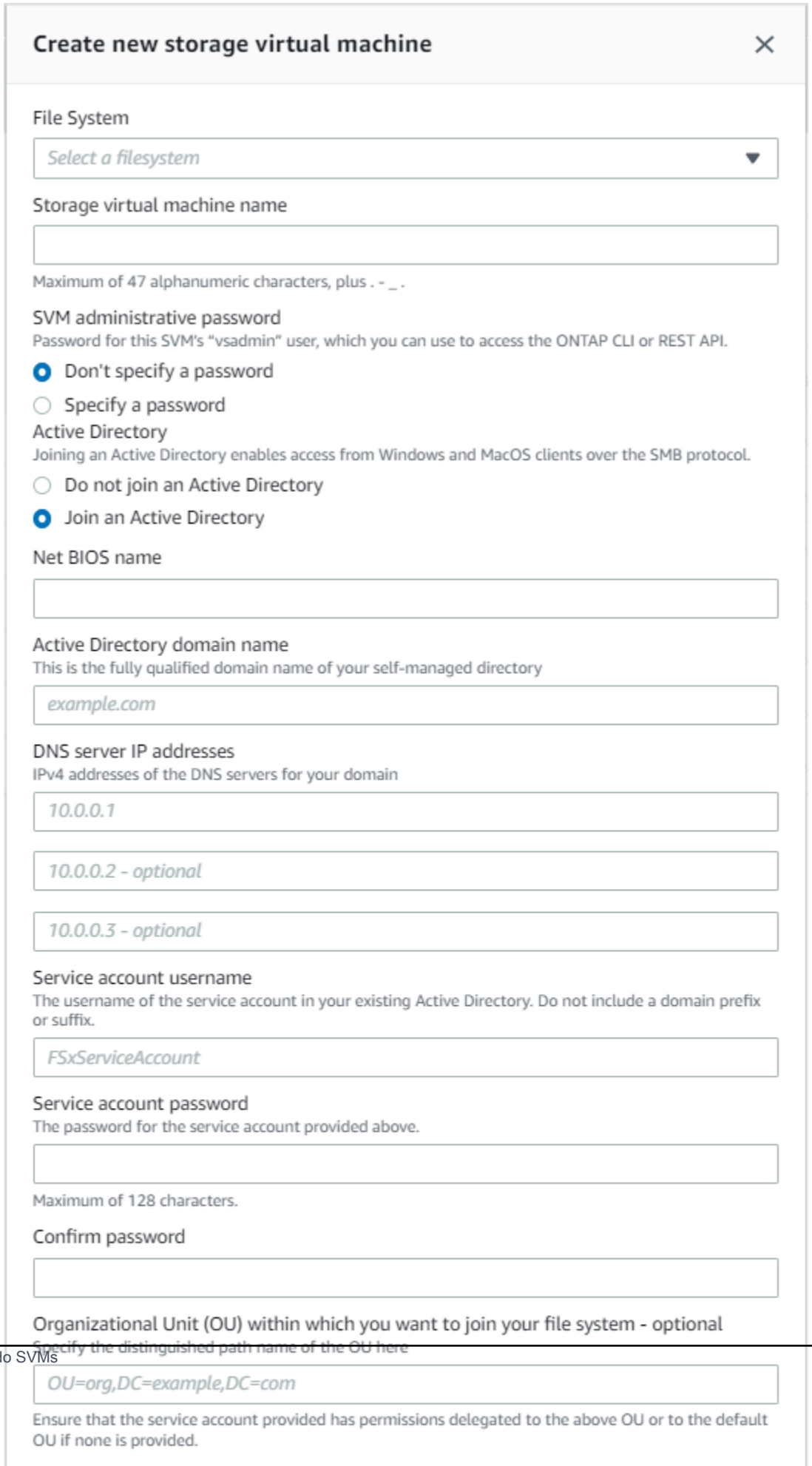
- O FSx para o sistema de arquivos ONTAP ao qual ele pertence.
- A configuração do Microsoft Active Directory (AD). Opcionalmente, você pode associar a SVM a um AD autogerenciado para fins de autenticação e controle de acesso de clientes Windows e macOS. Para obter mais informações, consulte Trabalhando com o Microsoft Active Directory no FSx ONTAP.

- O estilo de segurança do volume raiz — defina o estilo de segurança do volume raiz (Unix ou NTFS) de acordo com o tipo de clientes que você está usando para acessar seus dados no SVM. Para obter mais informações, consulte Estilo de segurança do volume.
- A senha administrativa da SVM. Opcionalmente, você pode definir a senha para o usuário `vsadmin` da SVM. Para obter mais informações, consulte Gerenciando SVMs com o ONTAP CLI.

Criar uma máquina virtual de armazenamento (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Máquinas virtuais de armazenamento.
3. Escolha Criar máquina virtual de armazenamento.

   A caixa de diálogo Criar máquina virtual de armazenamento é exibida.


Create new storage virtual machine
File System
Select a filesystem
Storage virtual machine name
Maximum of 47 alphanumeric characters, plus . - _ .
SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.
Don't specify a password
Specify a password
Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.
Do not join an Active Directory
Join an Active Directory
Net BIOS name
Active Directory domain name
This is the fully qualified domain name of your self-managed directory
example.com
DNS server IP addresses
IPv4 addresses of the DNS servers for your domain
10.0.0.1
10.0.0.2 - optional
10.0.0.3 - optional
Service account username
The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
FSxServiceAccount
Service account password
The password for the service account provided above.
Maximum of 128 characters.
Confirm password
Organizational Unit (OU) within which you want to join your file system - optional
Specify the distinguished path name of the OU here
OU=org,DC=example,DC=com
Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

4. Em Sistema de arquivos, escolha o sistema de arquivos no qual criar a máquina virtual de armazenamento.
5. No campo Nome da máquina virtual de armazenamento, forneça um nome para a máquina virtual de armazenamento. Você pode usar, no máximo, 47 caracteres alfanuméricos, além do caractere especial de sublinhado (_).
6. Em Senha administrativa da SVM, você pode, opcionalmente, escolher Especificar uma senha e fornecer uma senha para o usuário `vsadmin` dessa SVM. Você pode usar o usuário `vsadmin` para administrar a SVM utilizando a CLI ou a API REST do ONTAP. Para obter mais informações sobre o usuário `vsadmin`, consulte Gerenciando SVMs com o ONTAP CLI.

   Se você escolher Não especificar uma senha (o padrão), ainda poderá utilizar o usuário `fsxadmin` do sistema de arquivos para gerenciar o sistema usando a CLI ou a API REST do ONTAP, mas não poderá utilizar o usuário `vsadmin` da SVM para fazer o mesmo.
7. Em Active Directory, você tem as opções a seguir.

   - Se não estiver associando o sistema de arquivos a um Active Directory (AD), escolha Não associar um Active Directory.
   - Se estiver associando a SVM ao domínio de um AD autogerenciado, escolha Associar um Active Directory e forneça os detalhes a seguir para o AD. Para obter mais informações, consulte Pré-requisitos para unir uma SVM a um Microsoft AD autogerenciado.
     - O nome NetBIOS do objeto de computador do Active Directory que será criado para a SVM. O nome NetBIOS não pode ter mais de 15 caracteres. Esse é o nome dessa SVM no Active Directory.
     - O nome de domínio totalmente qualificado (FQDN) do Active Directory. O FQDN não pode exceder 255 caracteres.
     - Endereços IP do servidor DNS — Os IPv4 endereços dos servidores DNS do seu domínio.
     - Nome de usuário da conta de serviço: o nome de usuário da conta de serviço em seu Active Directory existente. Não inclua um prefixo ou sufixo de domínio. Para `EXAMPLE\ADMIN`, use `ADMIN`.
     - Senha da conta de serviço: a senha da conta de serviço.
     - Confirmar senha: a senha da conta de serviço.
     - (Opcional) Unidade organizacional (UO): o nome do caminho distinto da unidade organizacional à qual você deseja unir seu sistema de arquivos.
     - Grupo de administradores delegado do sistema de arquivos: o nome do grupo em seu AD que pode administrar seu sistema de arquivos.

Se você estiver usando AWS Managed Microsoft AD, deverá especificar um grupo como Administradores AWS Delegados, FSx Administradores AWS Delegados ou um grupo personalizado com permissões delegadas à OU.

Se você estiver ingressando em um AD autogerenciado, use o nome do grupo em seu AD. O grupo padrão é `Domain Admins`.

8. Em Estilo de segurança do volume raiz da SVM, escolha o estilo de segurança da SVM, dependendo do tipo de clientes que acessam seus dados. Escolha Unix (Linux) se clientes Linux são seu principal meio de acesso aos dados; escolha NTFS se clientes Windows são seu principal meio de acesso aos dados. Para obter mais informações, consulte Estilo de segurança do volume.
9. Escolha Confirmar para criar a máquina virtual de armazenamento.

Você pode monitorar o progresso da atualização na página de detalhes Sistemas de arquivos, na coluna Status do painel Máquinas virtuais de armazenamento. A máquina virtual de armazenamento estará pronta para uso quando o status for Criado.

Criar uma máquina virtual de armazenamento (CLI)

- Para criar uma máquina virtual de armazenamento (SVM) FSx para ONTAP, use o comando create-storage-virtual-machineCLI (ou a operação de CreateStorageVirtualMachineAPI equivalente), conforme mostrado no exemplo a seguir.

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name svm1 \
    --svm-admin-password password \
    --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Depois de criar com sucesso a máquina virtual de armazenamento, a Amazon FSx retorna sua descrição no formato JSON, conforme mostrado no exemplo a seguir.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
```

```
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Atualizar máquinas virtuais de armazenamento (SVM)

Você pode atualizar as seguintes propriedades de configuração da máquina virtual de armazenamento (SVM) usando o FSx console da Amazon e a FSx API da Amazon: AWS CLI

- Senha da conta administrativa da SVM.
- Configuração do Active Directory (AD) da SVM: você pode associar uma SVM a um AD ou modificar a configuração do AD de uma SVM já associada a um AD. Para obter mais informações, consulte Como gerenciar configurações do Active Directory para SVM.

Atualizar as credenciais da conta de administrador da SVM (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Escolha a SVM a ser atualizada da seguinte forma:
   - No painel de navegação à esquerda, escolha Sistemas de arquivos e selecione o sistema de arquivos do ONTAP para o qual deseja atualizar uma SVM.
   - Escolha a guia Máquinas virtuais de armazenamento.

     Ou

   - Para exibir uma lista de todos os SVMs disponíveis Conta da AWS na sua versão atual Região da AWS, expanda ONTAP e escolha Armazenamento de máquinas virtuais.
3. Escolha a máquina virtual de armazenamento que deseja atualizar.
4. Escolha Ações > Atualizar senha do administrador. A janela Atualizar credenciais administrativas da SVM é exibida.
5. Insira a nova senha do usuário `vsadmin` e confirme-a.
6. Escolha Atualizar credenciais para salvar a nova senha.

Atualizar as credenciais da conta de administrador da SVM (CLI)

- Para atualizar a configuração de um FSx para ONTAP SVM, use o comando update-storage-virtual-machineCLI (ou a operação de UpdateStorageVirtualMachineAPI equivalente), conforme mostrado no exemplo a seguir.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

Depois de criar com sucesso a máquina virtual de armazenamento, a Amazon FSx retorna sua descrição no formato JSON, conforme mostrado no exemplo a seguir.


```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
```

```
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
    "StorageVirtualMachineId": "svm-abcdef01234567890",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Auditar acesso a arquivos

O Amazon FSx for NetApp ONTAP oferece suporte à auditoria de acessos de usuários finais a arquivos e diretórios em uma máquina virtual de armazenamento (SVM).

Tópicos

- Visão geral da auditoria de acesso a arquivos
- Visão geral das tarefas para configurar a auditoria de acesso a arquivos

Visão geral da auditoria de acesso a arquivos

A auditoria de acesso a arquivos permite que você registre os acessos do usuário final a arquivos e diretórios individuais com base nas políticas de auditoria que você define. A auditoria de acesso a arquivos ajuda a melhorar a segurança do sistema e reduzir o risco de acesso não autorizado aos dados do sistema. A auditoria de acesso a arquivos ajuda as organizações a permanecerem em conformidade com os requisitos de proteção de dados, identificarem ameaças potenciais com antecedência e reduzirem o risco de uma violação de dados.

Em todos os acessos a arquivos e diretórios, a Amazon FSx suporta o registro de tentativas bem-sucedidas (como um usuário com permissões suficientes acessando um arquivo com sucesso), tentativas malsucedidas ou ambas. Você também pode desativar a auditoria de acesso a arquivos a qualquer momento.

Por padrão, os logs de eventos de auditoria são armazenados no formato de arquivo `EVTX`, o que permite visualizá-los usando o Microsoft Event Viewer.

Eventos de acesso SMB que podem ser auditados

A tabela a seguir lista os eventos de acesso a arquivos e pastas SMB que podem ser auditados.

ID do evento (EVT/ EVTX)	Event	Descrição	Categoria
560/4656	Abrir objeto/Criar objeto	ACESSO AO OBJETO: objeto (arquivo ou diretório) aberto	Acesso a arquivos
563/4659	Abrir objeto com a intenção de exclusão	ACESSO AO OBJETO: um identificador para um objeto (arquivo ou diretório) foi solicitado com a intenção de exclusão	Acesso a arquivos
564/4660	Excluir objeto	ACESSO AO OBJETO: excluir objeto (arquivo ou diretório) O ONTAP gera esse evento quando um cliente Windows tenta excluir o objeto (arquivo ou diretório)	Acesso a arquivos
567/4663	Leia os atributos Object/Write Object/	ACESSO AO OBJETO: tentativa	Acesso a arquivos

ID do evento (EVT/ EVTX)	Event	Descrição	Categoria
	Get Object Attributes/ Set do objeto	de acesso ao objeto (leitura, gravação, obtenção do atributo, definição do atributo). **Note** Para esse evento, o ONTAP audita somente a primeira operação de leitura e gravação SMB (êxito ou falha) em um objeto. Isso impede que o ONTAP crie entradas de logs excessivas quando um único cliente abre um objeto e executa várias operações sucessivas de leitura ou gravação	

ID do evento (EVT/EVTX)	Event	Descrição	Categoria
		no mesmo objeto.	
N/A/4664	Links físicos	ACESSO AO OBJETO: Foi feita uma tentativa de criar um link físico	Acesso a arquivos
ID 9999 do evento N/A/N/A do ONTAP	Renomear objeto	ACESSO AO OBJETO: objeto renomeado. Este é um evento do ONTAP. No momento, o Windows não oferece suporte como evento único.	Acesso a arquivos
ID 9998 do evento N/A/N/A do ONTAP	Desvincular objeto	ACESSO AO OBJETO: objeto desvinculado. Este é um evento do ONTAP. No momento, o Windows não oferece suporte como evento único.	Acesso a arquivos

Eventos de acesso ao NFS que podem ser auditados

Os eventos de acesso a arquivos e pastas NFS a seguir que podem ser auditados.

- READ
- OPEN
- CLOSE

- READDIR
- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

Visão geral das tarefas para configurar a auditoria de acesso a arquivos

A configuração FSx do ONTAP para auditoria de acesso a arquivos envolve as seguintes tarefas de alto nível:

1. Familiarize-se com os requisitos e considerações sobre auditoria de acesso a arquivos.
2. Crie uma configuração de auditoria em uma SVM específica.
3. Ative a auditoria nessa SVM.
4. Configure políticas de auditoria em seus arquivos e diretórios.
5. Visualize os registros de eventos de auditoria depois que FSx o ONTAP os emitir.

Os detalhes da tarefa são fornecidos nos procedimentos a seguir.

Repita as tarefas para qualquer outra SVM em seu sistema de arquivos para a qual você deseja habilitar a auditoria de acesso a arquivos.

Requisitos de auditoria

Antes de configurar e habilitar a auditoria em uma SVM, você deve estar ciente dos requisitos e considerações a seguir.

- A auditoria NFS suporta entradas de controle de acesso (ACEs) de auditoria designadas como tipou, que geram uma entrada de registro de auditoria quando há uma tentativa de acesso

ao objeto. Para auditoria NFS, não há mapeamento entre bits de modo e auditoria. ACEs Ao converter ACLs para bits de modo, as auditorias ACEs são ignoradas. Ao converter bits de modo em ACLs, a auditoria não ACEs é gerada.

- A auditoria depende da disponibilidade de espaço nos volumes de preparação. (Um volume de preparação é um volume dedicado criado pelo ONTAP para armazenar arquivos de preparação, que são arquivos binários intermediários em nós individuais, nos quais os registros de auditoria são armazenados antes da conversão em um formato de arquivo EVTX ou XML.) Você deve garantir que haja espaço suficiente para os volumes de preparação nas agregações que contêm volumes auditados.
- A auditoria depende de ter espaço disponível no volume que contém o diretório no qual os logs de eventos de auditoria convertidos são armazenados. Certifique-se de que haja espaço suficiente nos volumes usados para armazenar logs de eventos. Você pode especificar o número de logs de auditoria a serem retidos no diretório de auditoria usando o parâmetro `-rotate-limit` ao criar uma configuração de auditoria, o que pode ajudar a garantir que haja espaço disponível suficiente para os logs de auditoria no volume.

Criação de configurações de auditoria em SVMs

Antes de começar a auditar eventos de arquivos e diretórios, crie uma configuração de auditoria na máquina virtual de armazenamento (SVM). Depois de criar a configuração de auditoria, você deve habilitá-la na SVM.

Antes de usar o comando `vserver audit create` para criar a configuração de auditoria, certifique-se de ter criado um diretório para ser usado como destino dos logs e de que o diretório não tenha links simbólicos. Você especifica o diretório de destino com o parâmetro `-destination`.

Você pode criar uma configuração de auditoria que alterne os logs de auditoria com base no tamanho do log ou em uma programação, da seguinte maneira:

- Para alternar os logs de auditoria com base no tamanho do registro, use este comando:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

  O exemplo a seguir cria uma configuração de auditoria para a SVM chamada `svm1` que audita operações de arquivo e eventos de logon e logoff do CIFS (SMB) (o padrão) usando rotação baseada em tamanho. O formato de log é EVTX (o padrão), os logs são armazenados no diretório `/audit_log` e você terá um único arquivo de log por vez (até 200 MB de tamanho).

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- Para alternar os logs de auditoria com base em uma programação, use este comando:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]
       [-rotate-limit integer] [-rotate-schedule-month chron_month]
       [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-
day chron_dayofmonth]
       [-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

O parâmetro `-rotate-schedule-minute` será obrigatório se você estiver configurando a rotação de logs de auditoria com base no tempo.

O exemplo a seguir cria uma configuração de auditoria para a SVM chamada `svm2` usando rotação baseada em tempo. O formato do log é EVTX (o padrão) e os logs de auditoria são alternados mensalmente, às 12h30, todos os dias da semana.

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB  -
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -
rotate-schedule-minute 30
```

Você pode usar o parâmetro `-format` para especificar se os logs de auditoria são criados no formato EVTX convertido (o padrão) ou no formato de arquivo XML. O formato EVTX permite que você visualize os arquivos de log com o Microsoft Event Viewer.

Por padrão, as categorias de eventos a serem auditados são eventos de acesso a arquivos (SMB e NFS), eventos de logon e logoff do CIFS (SMB) e eventos de alteração da política de autorização. Você pode ter maior controle sobre quais eventos registrar pelo parâmetro `-events`, que tem o seguinte formato:

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-
account|authorization-policy-change|security-group}
```

Por exemplo, o uso de `-events file-share` permite a auditoria dos eventos de compartilhamento de arquivos.

Para obter mais informações sobre o comando `vserver audit create`, consulte Criar uma configuração de auditoria.

Ativação da auditoria em uma SVM

Depois de concluir a definição da configuração de auditoria, você deve habilitá-la na SVM. Para fazer isso, use o seguinte comando:

```
vserver audit enable -vserver svm_name
```

Por exemplo, use o comando a seguir para habilitar a auditoria na SVM chamada `svm1`.

```
vserver audit enable -vserver svm1
```

Você pode desabilitar a auditoria de acesso a qualquer momento. Por exemplo, use o comando a seguir para desativar a auditoria na SVM chamada `svm4`.

```
vserver audit disable -vserver svm4
```

Quando você desabilita a auditoria, a configuração de auditoria não é excluída na SVM, o que significa que você pode reabilitar a auditoria nessa SVM a qualquer momento.

Como configurar as políticas de auditoria de arquivos e pastas

Você precisa configurar as políticas de auditoria nos arquivos e pastas em que deseja auditar tentativas de acesso do usuário. Você pode configurar políticas de auditoria para monitorar as tentativas de acesso com êxito e falha.

É possível configurar as políticas de auditoria SMB e NFS. As políticas de auditoria SMB e NFS têm requisitos de configuração e recursos de auditoria diferentes com base no estilo de segurança do volume.

Políticas de auditoria em arquivos e diretórios no estilo de segurança NTFS

Você pode configurar políticas de auditoria NTFS usando a guia Segurança do Windows ou a CLI do ONTAP.

Para configurar políticas de auditoria NTFS (guia Segurança do Windows)

Você configura as políticas de auditoria do NTFS adicionando entradas ao NTFS associadas SACLs a um descritor de segurança NTFS. O descritor de segurança é então aplicado aos arquivos e diretórios NTFS. Essas tarefas são gerenciadas automaticamente pela GUI do Windows. O descritor de segurança pode conter listas de controle de acesso discricionárias (DACLs) para aplicar

permissões de acesso a arquivos e pastas, SACLs para auditoria de arquivos e pastas, ou ambos e. SACLs DACLs

1. No menu Ferramentas do Windows Explorer, selecione Mapear unidade de rede.
2. Preencha a caixa Mapear unidade de rede:

   a. Escolha uma letra de Unidade.
   b. Na caixa Pasta, digite o nome do servidor SMB (CIFS) que contém o compartilhamento, contendo os dados que você deseja auditar e o nome do compartilhamento.
   c. Escolha Terminar.

   A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.
3. Selecione o arquivo ou diretório cujo acesso de auditoria você deseja habilitar.
4. Clique com o botão direito do mouse no arquivo ou diretório e escolha Propriedades.
5. Escolha a guia Segurança.
6. Clique em Avançado.
7. Escolha a guia Auditoria.
8. Execute as ações desejadas:

Se você deseja...	Faça o seguinte
Configurar a auditoria para um novo usuário ou grupo	1. Escolha Adicionar. 2. Na caixa Digite o nome do objeto a ser selecionado, digite o nome do usuário ou grupo que você deseja adicionar. 3. Escolha OK.
Remover a auditoria de um usuário ou grupo	1. Na caixa Digite o nome do objeto a ser selecionado, selecione o usuário ou grupo que você deseja remover. 2. Escolha Remover. 3. Escolha OK. 4. Ignore o restante deste procedimento.
Alterar a auditoria de um usuário ou grupo	1. Na caixa Digite o nome do objeto a ser selecionado, escolha o usuário ou grupo que você deseja alterar.

Se você deseja...	Faça o seguinte
	2. Escolha Editar. 3. Escolha OK.

Se você estiver configurando a auditoria em um usuário ou grupo ou alterando a auditoria em um usuário ou grupo existente, a caixa Entrada de auditoria para ***object*** será aberta.

9. Na caixa Aplicar a, selecione como você deseja aplicar essa entrada de auditoria.

   Se você estiver configurando a auditoria em um único arquivo, a caixa Aplicar a não estará ativa, pois o padrão é Somente este objeto.

10. Na caixa Acesso, selecione o que você deseja auditar e se deseja auditar eventos com êxito, eventos de falha ou ambos.

    - Para auditar eventos com êxito, escolha a caixa Sucesso.
    - Para auditar eventos de falha, escolha a caixa Falha.

    Escolha as ações que você precisa monitorar para atender aos seus requisitos de segurança. Para obter mais informações sobre esses eventos auditáveis, consulte a documentação do Windows. Você pode auditar os seguintes eventos:

    - Controle total
    - Percorrer pasta/executar arquivo
    - Listar pasta//ler dados
    - Ler atributos
    - Ler atributos estendidos
    - Criar arquivos/gravar dados
    - Criar pastas/anexar dados
    - Gravar atributos
    - Gravar atributos estendidos
    - Excluir subpastas e arquivos
    - Excluir
    - Permissões de leitura

- Alterar permissões.
- Assumir a propriedade

11. Se você não quiser que a configuração de auditoria se propague para arquivos e pastas subsequentes do contêiner original, escolha a caixa Aplicar estas entradas de auditoria somente a objetos e/ou contêineres dentro deste contêiner.
12. Escolha Aplicar.
13. Ao terminar de adicionar, remover ou editar entradas de auditoria, escolha OK.

    A *object* caixa Entrada de Auditoria para fecha.
14. Na caixa Auditoria, escolha as configurações de herança para essa pasta. Escolha somente o nível mínimo que forneça os eventos de auditoria que atendam aos seus requisitos de segurança.

    Você pode escolher uma das seguintes opções:

    - Escolha a caixa Incluir entradas de auditoria herdáveis na entrada principal deste objeto.
    - Escolha a caixa Substituir todas as entradas de auditoria herdáveis existentes em todos os descendentes por entradas de auditoria herdáveis deste objeto.
    - Escolha as duas caixas.
    - Escolha nenhuma das caixas.

    Se você estiver configurando SACLs em um único arquivo, a caixa Substituir todas as entradas de auditoria herdadas existentes em todos os descendentes por entradas de auditoria herdadas desse objeto não estará presente na caixa Auditoria.
15. Escolha OK.

Configurar políticas de auditoria do NTFS (CLI do ONTAP)

Usando a CLI do ONTAP, você pode configurar políticas de auditoria do NTFS sem precisar se conectar aos dados usando um compartilhamento SMB em um cliente Windows.

- Você pode configurar políticas de auditoria do NTFS usando a família de comandos vserver security file-directory ntfs sacl add.

Por exemplo, o comando a seguir cria uma política de segurança com `p1` o nome do SVM. `vs0`

```
vserver security file-directory policy create -policy-name p1 -vserver vs0
```

Em seguida, o comando a seguir aplica a política de p1 segurança ao vs0 SVM.

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

Políticas de auditoria em arquivos e diretórios no estilo de segurança do UNIX

Você configura a auditoria para arquivos e diretórios no estilo de segurança do UNIX adicionando auditoria ACEs (expressões de controle de acesso) ao NFS v4.x (listas de controle de acesso). ACLs Isso permite monitorar determinados eventos de acesso a arquivos e diretórios NFS para fins de segurança.

> **Note**
>
> Para o NFS v4.x, tanto o sistema discricionário quanto o sistema ACEs são armazenados na mesma ACL. Portanto, você deve ter cuidado ao adicionar auditoria ACEs a uma ACL existente para evitar sobrescrever e perder uma ACL existente. A ordem na qual você adiciona a auditoria ACEs a uma ACL existente não importa.

Configurar políticas de auditoria do UNIX

1. Recupere a ACL existente para o arquivo ou diretório usando o comando `nfs4_getfacl` ou um equivalente.
2. Anexe a auditoria desejada. ACEs
3. Aplique a ACL atualizada ao arquivo ou diretório usando o comando `nfs4_setfacl` ou um equivalente.

   Este exemplo usa a opção `-a` para dar a um usuário (chamado `testuser`) permissões de leitura para o arquivo chamado `file1`.

   ```
   nfs4_setfacl -a "A::testuser@example.com:R" file1
   ```

Visualização de logs de evento de auditoria

Você pode visualizar os logs de evento de auditoria salvos nos formatos de arquivo EVTX ou XML.

- Formato de arquivo EVTX: você pode abrir os logs de evento de auditoria EVTX convertidos como arquivos salvos usando o Microsoft Event Viewer.

  Há duas opções que você pode usar ao visualizar logs de eventos usando o visualizador de eventos:

  - Visualização geral: as informações comuns a todos os eventos são exibidas no registro do evento. Os dados específicos do evento para o registro do evento não são exibidos. Você pode usar a visualização detalhada para exibir dados específicos do evento.
  - Visualização detalhada: uma visualização amigável e uma visualização em XML estão disponíveis. As visualizações amigável e em XML exibem as informações que são comuns a todos os eventos e os dados específicos do evento para o registro de eventos.
- Formato de arquivo XML: você pode visualizar e processar logs de evento de auditoria XML em aplicações de terceiros que aceitam o formato de arquivo XML. As ferramentas de visualização em XML podem ser usadas para visualizar os logs de auditoria, desde que você tenha o esquema XML e informações sobre as definições dos campos XML.

Configurando um servidor SMB em um grupo de trabalho

Você pode configurar um servidor Server Message Block (SMB) em um grupo de trabalho como alternativa à associação de uma SVM a um Microsoft Active Directory quando a infraestrutura de domínio do Microsoft Active Directory não estiver disponível. Um grupo de trabalho é uma peer-to-peer rede que usa o protocolo SMB e tem somente contas e grupos locais.

O processo de configuração de um servidor SMB como membro de um grupo de trabalho consiste no seguinte:

- Criando o servidor SMB em uma máquina virtual de armazenamento (SVM).
- Criação de usuários e grupos locais.
- Adicionar usuários ou grupos locais como membros do grupo de trabalho.

Lembre-se de que os servidores SMB no modo de grupo de trabalho não oferecem suporte aos seguintes recursos SMB:

- SMB3 Protocolo de testemunha
- SMB3 Ações da CA
- SQL sobre SMB

- Redirecionamento de pasta
- Perfis de roaming
- Objeto de política de grupo (GPO)
- Serviço de instantâneo de volume (VSS)

Além disso, um servidor SMB no modo de grupo de trabalho oferece suporte somente à autenticação NTLM e não à autenticação Kerberos.

Os procedimentos a seguir conduzem você pelo processo de configuração de um servidor SMB em um SVM em um grupo de trabalho, criar contas locais e adicionar essas contas à associação do grupo de trabalho. Você usará a NetApp ONTAP CLI do sistema de arquivos ou da interface de gerenciamento do SVM para implementar esses procedimentos. Para obter mais informações, consulte Usar o NetApp ONTAP CLI.

Tópicos

- Criando um servidor SMB em um grupo de trabalho
- Criação de uma conta de usuário local no servidor SMB
- Criação de grupos locais no servidor SMB
- Adicionar usuários locais ao grupo local

Criando um servidor SMB em um grupo de trabalho

Você pode usar o vserver cifs createONTAP CLIcomando para criar um servidor SMB no SVM e especificar o grupo de trabalho ao qual ele pertence.

Antes de começar

O SVM e os volumes (e interfaces) que você está usando para fornecer dados devem ter sido configurados para permitir o protocolo SMB.

O LIFs deve ser capaz de se conectar aos servidores DNS que estão configurados no SVM. Uma licença CIFS pode ser necessária no sistema de arquivos, no entanto, uma licença CIFS não é necessária se o servidor SMB for usado somente para autenticação.

Para criar um servidor SMB em um grupo de trabalho

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua

management_endpoint_ip pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Crie o servidor SMB em um grupo de trabalho:

```
FSxIdabcde123456::> vserver cifs create -vserver vserver_name -cifs-
server cifs_server_name -workgroup workgroup_name [-comment workgroup_description]
```

O comando a seguir cria o servidor SMB `smb_server01` no grupo de trabalho`workgroup01`:

```
FSxIdabcde123456::> vserver cifs create -vserver svm1 -cifs-server SMB_SERVER01 -
workgroup workgroup01
```

Se você estiver conectado à porta de gerenciamento do SVM, não precisará especificar a. `-vserver`

3. Verifique a configuração do servidor SMB usando o `vserver cifs show` comando.

No exemplo a seguir, a saída do comando mostra que um servidor SMB chamado `smb_server01` foi criado no SVM `svm1` no grupo de trabalho: `workgroup01`

```
FSxIdabcde123456::> vserver cifs show -vserver svm1

                                               Vserver: svm1
                            CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                     Fully Qualified Domain Name: -
                             Organizational Unit: -
    Default Site Used by LIFs Without Site Membership: -
                                     Workgroup Name: workgroup01
                                Authentication Style: workgroup
                  CIFS Server Administrative Status: up
                             CIFS Server Description:
                             List of NetBIOS Aliases: -
```

Criação de uma conta de usuário local no servidor SMB

Você pode criar uma conta de usuário local que pode ser usada para autorizar o acesso aos dados contidos no SVM por meio de uma conexão SMB. Você também pode usar contas de usuário locais para autenticação ao criar uma sessão SMB. A funcionalidade do usuário local é ativada por padrão quando o SVM é criado. Ao criar uma conta de usuário local, você deve especificar um nome de usuário e especificar o SVM ao qual associar a conta.

Para criar contas de usuário locais no servidor SMB

1. Crie o usuário local usando o comando vserver cifs users-and-groups local-user createONTAPCLI:

   ```
   vserver cifs users-and-groups local-user create -vserver svm_name -user-
   name user_name optional_parameters
   ```

   Os seguintes parâmetros opcionais podem ser úteis:

   - `-full-name`— O nome completo do usuário.
   - `-description`— Uma descrição para o usuário local.
   - `-is-account-disabled {true|false}`— Especifica se a conta do usuário está ativada ou desativada. Se esse parâmetro não for especificado, o padrão é ativar a conta do usuário.

   O comando solicita a senha do usuário local.
2. Insira uma senha para o usuário local e confirme a senha.
3. Verifique se o usuário foi criado com sucesso:

   ```
   vserver cifs users-and-groups local-user show -vserver svm_name
   ```

O exemplo a seguir cria um usuário local`SMB_SERVER01\sue`, com um nome completo`Sue Chang`, associado ao SVM: `svm1`

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user create -vserver svm1
 -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user show
Vserver  User Name                  Full Name  Description
-------- ------------------------- ---------- -------------
svm1     SMB_SERVER01\Administrator            Built-in administrator account
svm1     SMB_SERVER01\sue           Sue Chang
```

Criação de grupos locais no servidor SMB

Você pode criar grupos locais que podem ser usados para autorizar o acesso aos dados associados ao SVM por meio de uma conexão SMB. Você também pode atribuir privilégios que definem quais direitos ou capacidades de usuário um membro do grupo tem.

A funcionalidade de grupo local é ativada por padrão quando o SVM é criado. Ao criar um grupo local, você deve especificar um nome para o grupo e especificar o SVM ao qual associar o grupo. Você pode especificar um nome de grupo com ou sem o nome de domínio local e, opcionalmente, especificar uma descrição para o grupo local. Você não pode adicionar um grupo local a outro grupo local.

Para criar um grupo local no servidor SMB

1. crie o grupo local usando o comando vserver cifs users-and-groups local-group createONTAPCLI.

   ```
   vserver cifs users-and-groups local-group create -vserver svm_name -group-
   name group_name [-description local_group_description
   ```

   Incluir uma descrição para o grupo local é útil.
2. Verifique se o grupo foi criado com sucesso:

   ```
   vserver cifs users-and-groups local-group show -vserver svm_name
   ```

O exemplo a seguir cria um grupo local `SMB_SERVER01\engineering` associado ao SVM: `svm1`

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group create -vserver svm1 -
group-name SMB_SERVER01\engineering
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group show -vserver svm1
```

```
Vserver          Group Name                    Description
---------------- ----------------------------- ----------------------------
svm1             BUILTIN\Administrators        Built-in Administrators group
svm1             BUILTIN\Backup Operators      Backup Operators group
svm1             BUILTIN\Guests                Built-in Guests group
svm1             BUILTIN\Power Users           Restricted administrative privileges
svm1             BUILTIN\Users                 All users
svm1             SMB_SERVER01\engineering
```

Adicionar usuários locais ao grupo local

Você pode gerenciar a associação a grupos locais adicionando e removendo usuários locais ou de domínio, ou adicionando e removendo grupos de domínio. Isso é útil se você quiser controlar o acesso aos dados com base nos controles de acesso colocados no grupo ou se quiser que os usuários tenham privilégios associados a esse grupo. Se você não quiser mais que um usuário local, usuário de domínio ou grupo de domínio tenha direitos ou privilégios de acesso com base na associação a um grupo, você pode remover o membro do grupo.

Ao adicionar membros a um grupo local, tenha em mente o seguinte:

- Você não pode adicionar usuários ao grupo especial Todos.
- Você não pode adicionar um grupo local a outro grupo local.
- Para adicionar um usuário ou grupo de domínio a um grupo local, é ONTAP necessário poder resolver o nome para um SID.

Ao remover membros de um grupo local, lembre-se do seguinte:

- Você não pode remover membros do grupo especial Todos.
- Para remover um membro de um grupo local, ONTAP deve ser capaz de resolver seu nome para um SID.

Você precisa ter a `fsxadmin` função para executar os comandos usados neste procedimento. Para obter mais informações, consulte Usuários e perfis do ONTAP.

Para gerenciar a associação ao grupo local

- Adicione ou remova um membro de um grupo usando os comandos da CLI vserver cifs users-and-groups local-group add-memberse vserver cifs users-and-groups local-group ONTAP remove-members.

- Para adicionar membros a um grupo de trabalho:

```
vserver cifs users-and-groups local-group add-members -vserver svm_name -group-
name group_name -member-names name[,...]
```

  Você pode especificar uma lista delimitada por vírgula de usuários locais, usuários de domínio ou grupos de domínio para adicionar ao grupo local especificado.

- Para ver os membros de um grupo de trabalho:

```
vserver cifs users-and-groups local-group show-members -vserver svm_name -group-
name group_name
```

- Para remover membros de um grupo de trabalho:

```
vserver cifs users-and-groups local-group remove-members -vserver svm_name -
group-name group_name -member-names name[,...]
```

  Você pode especificar uma lista delimitada por vírgula de usuários locais, usuários de domínio ou grupos de domínio para remover do grupo local especificado.

O exemplo a seguir adiciona um usuário local SMB_SERVER01\sue ao grupo local SMB_SERVER01\engineering no SVM: svm1

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group add-members -vserver svm1
 -group-name SMB_SERVER01\engineering -member-names SMB_SERVER01\sue
```

O exemplo a seguir remove o usuário local SMB_SERVER01\sue e SMB_SERVER01\james do grupo local SMB_SERVER01\engineering no SVM: svm1

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group remove-
members -vserver svm1 -group-name SMB_SERVER01\engineering -member-names
 SMB_SERVER01\sue,SMB_SERVER01\james
```

O exemplo a seguir lista os membros do grupo localSMB_SERVER01\engineering:

```
FsxIdabcdef01234::> vserver cifs users-and-groups local-group show-members -
vserver svm_name -group-name group_name
```

```
            Vserver: svm1
        Domain Name: SMB_SERVER01
         Group Name: SMB_SERVER01\engineering
        Member Name: SMB_SERVER01\anita
                     SMB_SERVER01\james
                     SMB_SERVER01\liang
```

Detalhes de configuração da máquina virtual de armazenamento (SVM)

Você pode ver as máquinas virtuais FSx de armazenamento do ONTAP que estão atualmente em seu sistema de arquivos usando o FSx console da Amazon AWS CLI, o e a FSx API da Amazon.

Para visualizar uma máquina virtual de armazenamento no sistema de arquivos:

- Como usar o console: escolha um sistema de arquivos para visualizar a página de detalhes Sistemas de arquivos. Para listar todas as máquinas virtuais de armazenamento no sistema de arquivos, escolha a guia Máquinas virtuais de armazenamento e selecione a máquina virtual de armazenamento que deseja visualizar.
- Usando a CLI ou a API — Use o comando da describe-storage-virtual-machinesCLI ou a operação da API. DescribeStorageVirtualMachines

  A resposta do sistema é uma lista de descrições completas de tudo o que está SVMs em sua conta Região da AWS.

Excluir máquinas virtuais de armazenamento (SVM)

Você só pode excluir um FSx para o ONTAP SVM usando o FSx console da Amazon AWS CLI, o e a API. Antes de excluir uma SVM, você deve primeiro excluir todos os volumes não raiz anexados à SVM.

> **Important**
>
> Você não pode excluir uma SVM usando a NetApp CLI ou a API do ONTAP.

> **Note**
>
> Antes de excluir uma máquina virtual de armazenamento, verifique se nenhuma aplicação está acessando os dados na SVM e se você excluiu todos os volumes não raiz anexados à SVM.

Excluir uma máquina virtual de armazenamento (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Escolha a SVM que deseja excluir como mostrado a seguir.

   - No painel de navegação à esquerda, escolha Sistemas de arquivos e o sistema de arquivos do ONTAP do qual você deseja excluir uma SVM.
   - Escolha a guia Máquinas virtuais de armazenamento.

     Ou

   - Para exibir uma lista de todos os SVMs disponíveis, expanda ONTAP e escolha Armazenamento de máquinas virtuais.

   Na lista, selecione a SVM que deseja excluir.
3. Na guia Volumes, visualize a lista de volumes anexados à SVM. Se houver volumes não raiz anexados à SVM, é necessário excluí-los antes de excluir a SVM. Consulte Excluir volumes do para obter mais informações.
4. Escolha Excluir máquina virtual de armazenamento no menu Ações.
5. Na caixa de diálogo de confirmação da exclusão, escolha Excluir máquina virtual de armazenamento.

Excluir uma máquina virtual de armazenamento (CLI)

- Para excluir uma FSx máquina virtual de armazenamento do ONTAP, use o comando delete-storage-virtual-machineCLI (ou a operação de API DeleteStorageVirtualMachineequivalente), conforme mostrado no exemplo a seguir.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

Gerenciamento FSx de volumes ONTAP

Cada máquina virtual de armazenamento (SVM) em um sistema de arquivos FSx for ONTAP pode ter um ou mais volumes. Um volume é um contêiner de dados isolado para arquivos, diretórios ou unidades lógicas de armazenamento LUNs iSCSI (). Os volumes têm provisionamento reduzido, ou seja, consomem capacidade de armazenamento somente para os dados armazenados neles.

Você pode acessar um volume de clientes Linux, Windows ou macOS pelo protocolo Network File System (NFS), pelo protocolo Server Message Block (SMB) ou pelo protocolo Internet Small Computer Systems Interface (iSCSI) criando um LUN iSCSI (armazenamento em bloco compartilhado). FSx para ONTAP também suporta acesso multiprotocolo (acesso simultâneo a NFS e SMB) ao mesmo volume.

Você pode criar volumes usando o AWS Management Console, AWS CLI, a FSx API da Amazon ou NetApp BlueXP. Você também pode usar o endpoint administrativo do sistema de arquivos ou do SVM para criar, atualizar e excluir volumes usando o NetApp CLI do ONTAP ou API REST.

> **Note**
>
> Você pode criar 500 volumes por par de HA, até 1.000 volumes em todos os pares de HA. FlexGroup os volumes constituintes contam para esse limite. Por padrão, há oito volumes constituintes por agregado, por FlexGroup.

Ao criar um volume, defina as propriedades a seguir.

- Estilo de volume — O estilo de volume pode ser FlexVol or FlexGroup.
- Nome do volume: o nome do volume.
- Tipo do volume: o tipo do volume pode ser leitura e gravação (RW) ou proteção de dados (DP). Os volumes DP são somente para leitura e usados como destino em um NetApp SnapMirror or SnapVault relacionamento.
- Tamanho do volume: essa é a quantidade máxima de dados que o volume pode armazenar, independentemente do nível de armazenamento.
- Caminho da junção: esse é o local no namespace da SVM no qual o volume é montado.
- Eficiência de armazenamento: os recursos de eficiência de armazenamento, incluindo compactação, compressão e desduplicação de dados, proporcionam uma economia habitual de armazenamento de 65% para workloads de repositório de arquivos de uso geral.

- Estilo de segurança do volume (Unix ou NTFS): determina quais tipos de permissões são usados para acesso aos dados no volume ao autorizar usuários.
- Divisão de dados em camada: a política de camadas define quais dados são armazenados no nível econômico do grupo de capacidade.
- Período de resfriamento da política de camadas: define quando os dados são marcados como frios e movidos para o armazenamento do grupo de capacidade.
- Política de snapshots: as políticas de snapshots definem como o sistema cria snapshots para um volume. Você pode escolher entre três políticas predefinidas ou usar uma política personalizada que você criou usando a CLI ou a API REST do ONTAP.
- Copiar tags para backups — A Amazon FSx copiará automaticamente todas as tags de seus volumes para backups usando essa opção. Você pode definir essa opção usando a FSx API AWS CLI ou a Amazon.

Tópicos

- Estilos de volume
- Tipos de volume
- Estilo de segurança do volume
- Como criar volumes
- Atualizar volumes
- Mover volumes entre agregados
- Monitoramento de volumes
- Excluir volumes do

Estilos de volume

FSx for ONTAP oferece dois estilos de volumes que você pode usar para finalidades diferentes. Você pode criar um FlexVol ou mais FlexGroup volumes usando o FSx console da Amazon AWS CLI, o e a FSx API da Amazon.

- FlexVol os volumes oferecem a experiência mais simples para sistemas de arquivos com um par de alta disponibilidade (HA), portanto, são o estilo de volume padrão para sistemas de arquivos de primeira geração e sistemas de arquivos de segunda geração com um par de HA. O tamanho mínimo de um FlexVol o volume é de 20 mebibytes (MiB) e o tamanho máximo é 314.572.800 MiB.

- FlexGroup os volumes são compostos por vários constituintes FlexVol volumes, o que lhes permite oferecer maior desempenho e escalabilidade de armazenamento do que FlexVol volumes para sistemas de arquivos com vários pares de HA. FlexGroup volumes são o estilo de volume padrão para sistemas de arquivos de segunda geração com mais de um par de HA. O tamanho mínimo de um FlexGroup o volume é de 100 gibibytes (GiB) por componente e o tamanho máximo é de 20 pebibytes (PiB).

Você pode converter um volume com o FlexVol estilo para o FlexGroup estilo com o ONTAP CLI, que cria um FlexGroup com um único constituinte. No entanto, recomendamos que você use AWS DataSync para mover dados entre um FlexVol volume e um novo FlexGroup volume para garantir que os dados sejam distribuídos uniformemente pelo FlexGroup's constituintes. Para obter mais informações, consulte FlexGroup constituintes.

> **Note**
>
> Se você quiser usar o ONTAP CLI para converter um FlexVol volume para um FlexGroup volume, certifique-se de excluir todos os backups do FlexVol volume antes de convertê-lo. ONTAP não reequilibra automaticamente os dados como parte da conversão, portanto, os dados podem estar desequilibrados em todo o FlexGroup constituintes.

FlexGroup constituintes

A FlexGroup o volume é composto por constituintes, que são FlexVol volumes. Por padrão, FSx para ONTAP atribui oito constituintes a um FlexGroup volume por par de HA.

Quando você cria seu FlexGroup volume, seu tamanho é dividido uniformemente entre seus constituintes. Por exemplo, se você criar 800 gigabytes (GB) FlexGroup volume com oito constituintes, cada componente tem 100 GB de tamanho. A FlexGroup o volume pode ter entre 100 GB e 20 PiB, mas o tamanho total depende do tamanho dos constituintes. Cada componente tem um tamanho mínimo de 100 GB e máximo de 300 TiB. Por exemplo, um FlexGroup um volume com oito componentes tem um tamanho mínimo de 800 GB e um tamanho máximo de 20 PiB.

O ONTAP distribui dados entre os constituintes no nível de arquivo. Você pode armazenar até dois bilhões de arquivos em cada componente do seu FlexGroup volume.

Quando você atualiza o tamanho do seu FlexGroup volume, o novo tamanho é distribuído uniformemente entre seus constituintes existentes.

Você também pode adicionar mais constituintes ao seu FlexGroup volume usando o ONTAP CLI ou API REST. No entanto, recomendamos que faça isso somente se precisar de capacidade adicional de armazenamento e todos os seus componentes já estiverem no tamanho máximo (300 TiB por componente). A adição de componentes pode levar a um desequilíbrio de dados e E/S entre os componentes. Até que os constituintes estejam balanceados, é possível que a taxa de transferência de gravação seja 5— 10% menor do que uma balanceada FlexGroup volume. Quando novos dados são gravados no FlexGroup volume, o ONTAP prioriza distribuí-lo entre os novos constituintes até que os constituintes estejam equilibrados. Se você adicionar novos constituintes, recomendamos escolher um número par e não exceder a quantidade de oito por agregado.

> **Note**
>
> Se você adicionar novos constituintes, seus instantâneos existentes se tornarão instantâneos parciais; portanto, eles não poderão ser usados para restaurar totalmente seu FlexGroup volume para um estado anterior. Os instantâneos anteriores não podem oferecer uma point-in-time imagem completa do seu FlexGroup volume porque os novos constituintes ainda não existiam. No entanto, os instantâneos parciais podem ser usados para restaurar arquivos e diretórios individuais, criar um novo volume ou replicar com SnapMirror.

Tipos de volume

FSx for ONTAP oferece dois tipos de volumes que você pode criar usando o FSx console da Amazon AWS CLI, o e a FSx API da Amazon.

- Os volumes de leitura e gravação (RW) são usados na maioria dos casos. Como o nome indica, eles podem ser lidos e gravados.
- Os volumes de proteção de dados (DP) são volumes somente para leitura que você usa como destino de um NetApp SnapMirror or SnapVault relacionamento. Você deve usar os volumes DP quando quiser migrar ou proteger os dados de um único volume.

FlexVol and FlexGroup os volumes podem ser RW ou DP.

> **Note**
>
> Não é possível atualizar o tipo de um volume após a criação do volume.

Estilo de segurança do volume

Ao criar um volume FSx para ONTAP, você pode escolher entre dois estilos de segurança: Unix e NTFS. Cada estilo de segurança tem um efeito diferente na forma como as permissões são tratadas para os dados. É necessário entender os diferentes efeitos para garantir a seleção do estilo de segurança adequado aos seus propósitos.

É importante entender que os estilos de segurança não determinam quais tipos de clientes podem ou não acessar os dados. Os estilos de segurança determinam apenas o tipo de permissões FSx que o ONTAP usa para controlar o acesso aos dados e qual tipo de cliente pode modificar essas permissões.

Os dois fatores usados para determinar o estilo de segurança de um volume são o tipo de administrador que gerencia o sistema de arquivos e os tipos de usuários ou serviços que acessam os dados no volume.

Ao criar um volume no FSx console, na CLI e na API da Amazon, o estilo de segurança é automaticamente definido como o estilo de segurança do volume raiz. Você pode modificar o estilo de segurança de um volume usando a API AWS CLI ou. É possível modificar essa configuração após a criação do volume. Consulte Atualizar volumes para obter mais informações.

Ao configurar o estilo de segurança em um volume, considere as necessidades do seu ambiente para garantir que você selecione o melhor estilo de segurança para evitar problemas com o gerenciamento de permissões. Tenha em mente que o estilo de segurança não determina quais tipos de clientes podem acessar os dados. O estilo de segurança determina as permissões usadas para permitir o acesso aos dados e os tipos de clientes que podem modificar essas permissões. Veja a seguir algumas considerações que podem ajudar você a decidir qual estilo de segurança escolher para um volume.

- Unix (Linux): escolha esse estilo de segurança se o sistema de arquivos for gerenciado por um administrador do Unix, se a maioria dos usuários for de clientes NFS e se uma aplicação acessando os dados usar um usuário do Unix como conta de serviço. Somente clientes Linux podem modificar permissões com o estilo de segurança Unix, e os tipos de permissões usados em arquivos e diretórios são mode-bits ou NFS v4.x. ACLs
- NTFS: escolha esse estilo de segurança se o sistema de arquivos for gerenciado por um administrador do Windows, se a maioria dos usuários for de clientes SMB e se uma aplicação acessando os dados usar um usuário do Windows como conta de serviço. Se for necessário qualquer acesso do Windows a um volume, recomendamos usar o estilo de segurança NTFS.

Somente clientes Windows podem modificar permissões com o estilo de segurança NTFS, e os tipos de permissões usados em arquivos e diretórios são NTFS. ACLs

Como criar volumes

Você pode criar um FSx para ONTAP FlexVol or FlexGroup volume usando o FSx console da Amazon AWS CLI, o e a FSx API da Amazon, além do NetApp Interface de linha de comando (CLI) e API REST do ONTAP.

Para criar um FlexVol volume (console)

> **Note**
>
> O estilo de segurança do volume é automaticamente definido como o estilo de segurança do volume raiz.

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, selecione Volumes.
3. Escolha Create volume (Criar volume).
4. Em Tipo de sistema de arquivos, escolha Amazon FSx para NetApp ONTAP.
5. Forneça as seguintes informações na seção Detalhes do sistema de arquivos:
   - Em Sistema de arquivos, escolha o sistema de arquivos no qual criar o volume.
   - Em Máquina virtual de armazenamento, escolha a máquina virtual de armazenamento (SVM) na qual criar o volume.
6. Na seção Estilo de volume, escolha FlexVol.
7. Forneça as seguintes informações na seção Detalhes do volume:
   - No campo Nome do volume, forneça um nome para o volume. Você pode usar até 203 caracteres alfanuméricos ou sublinhado (_).
   - Em Tamanho do volume, insira qualquer número inteiro no intervalo de 20 a 314572800 para especificar o tamanho em mebibytes (MiB).
   - Para Tipo de volume, escolha Leitura-Gravação (RW) para criar um volume que seja legível e gravável ou Proteção de Dados (DP) para criar um volume que seja somente para leitura e

possa ser usado como destino de um NetApp SnapMirror or SnapVault relacionamento. Para obter mais informações, consulte Tipos de volume.

- Em Caminho da junção, insira um local no sistema de arquivos para montar o volume. O nome deve ter uma barra inicial, por exemplo `/vol3`.
- Em Eficiência de armazenamento, escolha Habilitado para habilitar os recursos de eficiência de armazenamento do ONTAP (desduplicação, compressão e compactação) nesse volume. Para obter mais informações, consulte Eficiência de armazenamento.
- Para o estilo de segurança de volume, escolha entre Unix (Linux) e NTFS para o volume. Para obter mais informações, consulte Estilo de segurança do volume.
- Em Política de snapshots, escolha uma política de snapshots para o volume. Para obter mais informações sobre políticas de snapshots, consulte Políticas de snapshots.

  Se você escolher Política personalizada, especifique o nome da política no campo política personalizada. A política personalizada já deve existir na SVM ou no sistema de arquivos. Você pode criar uma política de snapshots personalizada com a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política de snapshot no NetApp Documentação do produto ONTAP.

8. Na seção Armazenamento em camadas, forneça as seguintes informações.

   - Em Política de definição de níveis do grupo de capacidade, escolha a política de divisão em níveis do grupo de armazenamento para o volume, que pode ser Automática (o padrão), Somente snapshot, Todos ou Nenhuma. Para obter mais informações, consulte Políticas de camadas de volume.
   - Se escolher Automática ou Somente snapshot, você poderá definir o Período de resfriamento da política de divisão em níveis para definir o número de dias antes que os dados que não foram acessados sejam marcados como frios e movidos para o armazenamento do grupo de capacidade. É possível informar um valor entre 2 e 183 dias. A configuração padrão é de 31 dias.

9. Na seção Avançado, para SnapLock Configuração, escolha entre Ativado e Desativado. Para obter mais informações sobre como configurar um SnapLock Volume de conformidade ou um SnapLock Volume corporativo, consulte Noções básicas SnapLock Compliance Noções básicas SnapLock Enterprise e. Para obter mais informações sobre SnapLock, consulte Protegendo seus dados com SnapLock.
10. Escolha Confirmar para criar o volume.

Você pode monitorar o progresso da atualização na página de detalhes Sistemas de arquivos, na coluna Status do painel Volumes. O volume estará pronto para uso quando o status for Criado.

Para criar um FlexGroup volume (console)

> **Note**
>
> Você só pode criar FlexGroup volumes para sistemas de arquivos com vários pares de HA usando o FSx console da Amazon. Para criar FlexVol volumes para sistemas de arquivos com vários pares de HA, use a AWS CLI FSx API da Amazon ou ferramentas NetApp de gerenciamento.

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, selecione Volumes.
3. Escolha Create volume (Criar volume).
4. Em Tipo de sistema de arquivos, escolha Amazon FSx para NetApp ONTAP.
5. Forneça as seguintes informações na seção Detalhes do sistema de arquivos:
   - Em Sistema de arquivos, escolha o sistema de arquivos no qual criar o volume.
   - Em Máquina virtual de armazenamento, escolha a máquina virtual de armazenamento (SVM) na qual criar o volume.
6. Na seção Estilo de volume, escolha FlexGroup.
7. Forneça as seguintes informações na seção Detalhes do volume:
   - No campo Nome do volume, forneça um nome para o volume. Você pode usar até 203 caracteres alfanuméricos ou sublinhado (_).
   - Em Tamanho do volume, insira qualquer número inteiro de 800 gibibytes (GiB) a 2.400 tebibytes (TiB) por par de HA. Por exemplo, um sistema de arquivos com 12 pares de alta disponibilidade (HA) teria um tamanho mínimo de volume de 9.600 GiB e um tamanho máximo de 20.480 TiB.
   - Para Tipo de volume, escolha Leitura-Gravação (RW) para criar um volume que seja legível e gravável ou Proteção de Dados (DP) para criar um volume que seja somente para leitura e possa ser usado como destino de um NetApp SnapMirror or SnapVault relacionamento. Para obter mais informações, consulte Tipos de volume.

- Em Caminho da junção, insira um local no sistema de arquivos para montar o volume. O nome deve ter uma barra inicial, por exemplo `/vol3`.
- Para Eficiência de armazenamento, escolha Habilitado para habilitar os recursos de eficiência de armazenamento do ONTAP (eliminação da duplicação, compressão e compactação). Para obter mais informações, consulte Eficiência de armazenamento.
- Para o estilo de segurança de volume, escolha entre Unix (Linux) e NTFS para o volume. Para obter mais informações, consulte Estilo de segurança do volume.

> **Note**
>
> O estilo de segurança do volume é automaticamente definido como o estilo de segurança do volume raiz.

- Em Política de snapshots, escolha uma política de snapshots para o volume. Para obter mais informações sobre políticas de snapshots, consulte Políticas de snapshots.

  Se você escolher Política personalizada, especifique o nome da política no campo política personalizada. A política personalizada já deve existir na SVM ou no sistema de arquivos. Você pode criar uma política de snapshots personalizada com a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política de snapshot no NetApp Documentação do produto ONTAP.

8. Na seção Armazenamento em camadas, forneça as seguintes informações.

   - Em Política de definição de níveis do grupo de capacidade, escolha a política de divisão em níveis do grupo de armazenamento para o volume, que pode ser Automática (o padrão), Somente snapshot, Todos ou Nenhuma. Para obter mais informações, consulte Políticas de camadas de volume.
   - Se escolher Automática ou Somente snapshot, você poderá definir o Período de resfriamento da política de divisão em níveis para definir o número de dias antes que os dados que não foram acessados sejam marcados como frios e movidos para o armazenamento do grupo de capacidade. Você pode fornecer um valor entre 2 e 183 dias. A configuração padrão é de 31 dias.

9. Na seção Avançado, para SnapLock Configuração, escolha entre Ativado e Desativado. Para obter mais informações sobre como configurar um SnapLock Volume de conformidade ou um SnapLock Volume corporativo, consulte Noções básicas SnapLock Compliance Noções básicas

SnapLock Enterprise e. Para obter mais informações sobre SnapLock, consulte Protegendo seus dados com SnapLock.

10. Escolha Confirmar para criar o volume.

Você pode monitorar o progresso da atualização na página de detalhes Sistemas de arquivos, na coluna Status do painel Volumes. O volume estará pronto para uso quando o status for Criado.

Para criar um volume (CLI)

- Para criar um volume FSx for ONTAP, use o comando da CLI create-volume (ou a operação de API CreateVolumeequivalente), conforme mostrado no exemplo a seguir.

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
          SizeInMegabytes=1024,SnapshotPolicy=default, \
          StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
          StorageEfficiencyEnabled=true
```

Depois de criar o volume com sucesso, a Amazon FSx retorna sua descrição no formato JSON, conforme mostrado no exemplo a seguir.

```
{
    "Volume": {
        "CreationTime": "2022-08-12T13:03:37.625000-04:00",
        "FileSystemId": "fs-abcdef0123456789c",
        "Lifecycle": "CREATING",
        "Name": "vol1",
        "OntapConfiguration": {
            "CopyTagsToBackups": true,
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "NTFS",
            "SizeInMegabytes": 1024,
            "SnapshotPolicy": "default",
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abcdef0123456789a",
            "StorageVirtualMachineRoot": false,
```

```
            "TieringPolicy": {
                "Name": "NONE"
            },
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
        "VolumeId": "fsvol-abcdef0123456789b",
        "VolumeType": "ONTAP"


    }
}
```

Você também pode criar um novo volume restaurando um backup de um volume em um novo volume. Para obter mais informações, consulte Restaurar backups em um novo volume.

Atualizar volumes

Você pode atualizar a configuração de um volume FSx for ONTAP usando o FSx console da Amazon AWS CLI, o e a FSx API da Amazon, além do NetApp Interface de linha de comando (CLI) e API REST do ONTAP. Você pode modificar as seguintes propriedades de um volume existente FSx para ONTAP:

- Nome do volume
- Caminho da junção
- Tamanho do volume
- Eficiência de armazenamento
- Política de divisão em níveis do grupo de capacidade
- Estilo de segurança do volume
- Política de snapshots
- Período de resfriamento da política de divisão em níveis
- Copie tags para backups (usando AWS CLI a FSx API da Amazon)

Para obter mais informações, consulte Gerenciamento FSx de volumes ONTAP.

Para atualizar a configuração de um volume (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do ONTAP para o qual deseja atualizar um volume.
3. Escolha a guia Volumes.
4. Escolha o volume que deseja atualizar.
5. Em Ações, escolha Atualizar volume.

   A caixa de diálogo Atualizar volume é exibida com as configurações atuais do volume.
6. Em Caminho da junção, insira um local existente no sistema de arquivos para montar o volume. O nome deve ter uma barra inicial, como `/vol5`.
7. Para Tamanho do volume, você pode aumentar ou diminuir o tamanho do volume dentro do intervalo especificado no FSx console da Amazon. Para FlexVol volumes, o tamanho máximo é 300 TiB. Para FlexGroup volumes, o tamanho máximo é 300 TiB multiplicado pelo número total de volumes constituintes que seu FlexGroup tem até um máximo de 20 PiB.
8. Em Eficiência do armazenamento, escolha Habilitado para habilitar os recursos de eficiência de armazenamento do ONTAP (desduplicação, compressão e compactação), ou escolha Desabilitado para desabilitá-los.
9. Em Política de divisão em níveis do grupo de capacidade, escolha uma nova política de divisão em níveis do grupo de armazenamento para o volume, que pode ser Automática (o padrão), Somente snapshot, Todos ou Nenhuma. Para obter mais informações sobre políticas de camadas do grupo de capacidade, consulte Políticas de camadas de volume.
10. Em Estilo de segurança do volume, escolha Unix (Linux), NTFS ou Misto. O estilo de segurança de um volume determina se é dada preferência ao NTFS ou ao UNIX ACLs para acesso multiprotocolo. O modo MISTO não é necessário para acesso multiprotocolo e só é recomendado para usuários avançados.
11. Em Política de snapshots, escolha uma política de snapshots para o volume. Para obter mais informações sobre políticas de snapshots, consulte Políticas de snapshots.

    Se você escolher Política personalizada, especifique o nome da política no campo política personalizada. A política personalizada já deve existir na SVM ou no sistema de arquivos. Você pode criar uma política de snapshots personalizada com a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política de snapshot no NetApp Documentação do produto ONTAP.

12. Em Período de resfriamento da política de divisão em níveis, os valores válidos são de 2 a 183 dias. O período de resfriamento da política de camadas de um volume define o número de dias antes que os dados que não foram acessados sejam marcados como frios e movidos para o armazenamento do grupo de capacidade. Essa configuração afeta somente as políticas `Auto` e `Snapshot-only`.
13. Selecione Atualizar para atualizar o volume.

Atualizar a configuração de um volume (CLI)

- Para atualizar a configuração de um volume FSx for ONTAP, use o comando da CLI update-volume (ou a operação de API UpdateVolumeequivalente), conforme mostrado no exemplo a seguir.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Expandindo FlexGroup volumes

Você pode adicionar volumes adicionais de constituintes ao seu FlexGroup volume com o `volume expand` comando no ONTAP CLI. Essa é uma prática recomendada depois de adicionar pares de alta disponibilidade (HA) ao seu sistema de arquivos, pois garante que seu FlexGroup o volume permanece equilibrado.

Antes de expandir seu FlexGroup volume, considere os seguintes pontos:

- Tudo de um FlexGroup's volumes constituintes têm a mesma capacidade de armazenamento. Quando você expande seu FlexGroup volume com componentes adicionais, cada componente tem o mesmo tamanho que os constituintes existentes. Portanto, antes de adicionar os constituintes certifique-se de que cada agregado tenha espaço suficiente disponível.
- AWS recomenda manter oito volumes constituintes por agregado para cada FlexGroup volume. Oito volumes constituintes por agregado maximizam o paralelismo de FlexGroup volumes e oferece o melhor desempenho para sua carga de trabalho. Geralmente, recomendamos apenas

expandir seu FlexGroup volume com constituintes adicionais se você adicionar pares de HA. Esse é o único cenário em que você precisaria adicionar constituintes para manter oito constituintes por agregado.

- Se suas receitas FlexGroup o volume está em um SnapMirror relacionamento, depois a origem e o destino FlexGroup os volumes precisam ter o mesmo número de constituintes. Caso contrário, SnapMirror as transferências falharão. SnapMirror opera no nível constituinte e transfere dados entre cada constituinte individual. Portanto, se você expandir um FlexGroup volume com volumes constituintes adicionais, você também deve expandir manualmente qualquer volume que esteja em um SnapMirror relacionamento com ele.
- Quando você expande um FlexGroup volume com componentes adicionais, todas as cópias instantâneas existentes se tornam cópias “parciais”. Não é possível restaurar cópias parciais, mas é possível pesquisá-las e restaurar os arquivos individuais. Além disso, isso resulta na perda de qualquer incrementalidade para FSx backups, AWS backups ou SnapMirror relacionamentos.
- Você não poderá remover os volumes constituintes após adicioná-los.

Adicionando FlexGroup constituintes de volume

Você pode usar o ONTAP CLI para adicionar volumes constituintes ao seu FlexGroup volume.

Para adicionar FlexGroup constituintes de volume

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos FSx Amazon NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.
2. Use a expansão do volume ONTAP Comando CLI para expandir seu FlexGroup volume com constituintes adicionais. Substitua os valores a seguir:

   - `svm_name`com o nome da máquina virtual de armazenamento (SVM) que hospeda seu FlexGroup volume (por exemplo,`svm1`).
   - `vol_name`com o nome do FlexGroup volume que você deseja expandir (por exemplo,`vol1`).

- `aggregates`com uma lista separada por vírgulas dos agregados que você deseja adicionar FlexGroup volumes constituintes em. Por exemplo, `aggr1` para um único agregado ou `aggr1,aggr2` para vários agregados.
- O `constituent_per_aggregate` com o número de constituintes adicionais que você deseja adicionar a cada um dos `aggregates` especificados. Você só deve adicionar constituintes suficientes para garantir que seu FlexGroup o volume tem um número equilibrado de constituintes nos agregados em que reside.

```
::> volume expand -vserver svm_name -volume vol_name -aggr-list aggregates -aggr-
list-multiplier constituents_per_aggregate
```

> **Important**
>
> Você não pode remover FlexGroup constituintes depois de adicioná-los, então verifique suas entradas antes de executar o comando anterior.

Mover volumes entre agregados

Ao adicionar pares de alta disponibilidade (HA) ao seu sistema de arquivos, você precisa reequilibrar os dados existentes movendo os volumes para os novos agregados. Para mover um volume entre agregados, você pode usar o comando `volume move` na CLI do ONTAP.

Antes de usar o comando `volume move`, considere os seguintes pontos:

- O uso do comando `volume move` pode afetar o desempenho porque ele consome recursos de rede e disco em seu sistema de arquivos. Portanto, recomendamos mover volumes entre agregados durante períodos de baixa atividade. Como alternativa, ao mover volumes você pode reduzir a utilização do throughput da rede e a utilização do throughput de disco em seu sistema de arquivos para um volume que não seja superior a 50%.
- Para reduzir o impacto sobre o desempenho do seu sistema de arquivos, recomendamos mover um único volume entre dois pares de HA e agregados por vez. Por exemplo, se seu sistema de arquivos tiver quatro pares de HA, recomendamos mover dois volumes por vez (supondo que os movimentos de volume não sejam de ou para os mesmos pares de HA). O ONTAP é compatível com a movimentação de até oito volumes em cada par de HA por vez, porém, mais

movimentações simultâneas de volume reduzirão o desempenho de E/S do cliente e de qualquer movimentação de volume em andamento.

- Todos os dados armazenados na camada SSD do volume afetado são movidos fisicamente para um conjunto diferente de discos em um servidor de arquivos diferente. Essa operação ocorre em segundo plano e leva tempo. A taxa de tempo que a transferência leva dependerá da capacidade de throughput do sistema de arquivos e da quantidade de atividade no sistema de arquivos. No entanto, é possível realizar o controle de utilização para o movimento do volume. Para obter mais informações, consulte Realizar controle de utilização em movimentações de volume.
- Todos os dados armazenados no nível de capacidade não são movidos fisicamente porque os pares de HA compartilham o mesmo armazenamento do grupo de capacidade. Como resultado, a movimentação de volumes com a maioria dos dados em camadas será mais rápida. Lembre-se de que os metadados do arquivo sempre são armazenados no nível SSD. Para obter mais informações, consulte Divisão de dados em níveis no volume.

Fases da movimentação de um volume

Uma operação de movimentação de volume tem duas fases: a fase de replicação e a fase de substituição. Durante a fase de replicação, os dados existentes são replicados para o novo agregado do volume. Durante a fase de substituição, o ONTAP tenta fazer uma transferência rápida final para o novo agregado do volume. Isso inclui transferir todos os dados que foram gravados durante a fase de transferência e redirecionar o novo tráfego para o novo agregado do volume. Por padrão, a janela de substituição é de 30 segundos e interrompe toda a E/S do seu volume. Se o ONTAP não puder executar todas essas etapas durante a janela de substituição, ele falhará. Por padrão, o ONTAP tentará realizar a substituição três vezes consecutivas. Se as três tentativas consecutivas falharem, o ONTAP tentará novamente uma vez por hora até que seja bem-sucedido. Você pode reduzir a carga em seu sistema de arquivos para garantir que a fase de substituição seja bem-sucedida reduzindo ou pausando o tráfego de E/S para o volume antes do início da fase de substituição.

Iniciar movimentos de volume

Para iniciar um movimento de volume

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos FSx Amazon NetApp for ONTAP executando o seguinte comando. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Execute o comando volume move start na CLI do ONTAP. Substitua os valores a seguir:

   - O `vserver_name` com o nome do SVM que hospeda o volume que você está movendo.
   - O `volume_name` com o nome do componente do volume (por exemplo, `vol1__0001`).
   - O `aggregate_name` com o nome do agregado de destino para o volume.
   - O `-enforce-network-throttling` para acelerar o throughput total da movimentação de volume. Isso é opcional.

```
::> volume move start -vserver svm_name -volume volume_name --destination-
aggregate aggregate_name -foreground false
[Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".
 Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the
 status of this operation.
```

> **Important**
>
> A movimentação de volume consome recursos de rede e disco para os servidores de arquivos de origem e de destino. Portanto, o desempenho da sua workload pode ser afetado por qualquer movimentação de volume em andamento. Além disso, seu tráfego de E/S para o volume será pausado temporariamente durante a fase de substituição da movimentação do volume.

Monitorar movimentações de volume

Para monitorar uma movimentação de volume

- Para verificar o status da operação de movimentação de volume, use o comando `volume move show` da CLI do ONTAP.

```
::> volume move show -vserver svm_name -volume volume_name
```

```
Vserver Name: svm01
Volume Name: vol1__0001
Actual Completion Time: -
Bytes Remaining: 1.00TB
Specified Action For Cutover: retry_on_failure
Specified Cutover Time Window: 30
Destination Aggregate: aggr2
Destination Node: FsxId01234567890abcdef-03
Detailed Status: Transferring data: 12.23GB sent.
Percentage Complete: 1%
Move Phase: replicating
Prior Issues Encountered: -
Estimated Remaining Duration: 00:40:25
Replication Throughput: 434.3MB/s
Duration of Move: 00:00:27
Source Aggregate: aggr1
Source Node: FsxId01234567890abcdef-01
Move State: healthy
```

A saída do comando mostra a estimativa de tempo para concluir a movimentação. Após a conclusão, `Move phase` mostrará o status `completed`.

Mantendo o equilíbrio FlexGroup volumes

Para que sua carga de trabalho tenha um desempenho ideal, seu FlexGroup os volumes devem abranger todos os agregados e ter um número par de volumes constituintes por agregado. Recomendamos ter oito constituintes por agregado. Considere os seguintes cenários ao rebalancear FlexGroup volumes:

- Movendo-se FlexGroup constituintes entre agregados existentes: Se você mover um FlexGroup's volume constituinte para outro agregado de outra forma balanceado FlexGroup, você deve então mover outro componente menos utilizado para o agregado original. Isso garante que seu FlexGroup tem um número par de constituintes por agregado.

  Movendo-se FlexGroup constituintes em novos agregados após adicionar pares de HA: Se você mover um FlexGroup's volumes constituintes para novos agregados após adicionar pares de HA, então você deve expandir o FlexGroup com constituintes adicionais nos agregados que perderam constituintes. Isso garante que seu FlexGroup tem um número par de constituintes por agregado. Para obter mais informações, consulte the section called “Expandindo FlexGroup volumes”.

Realizar controle de utilização em movimentações de volume

Se quiser limitar a largura de banda de uma movimentação de volume em seu sistema de arquivos, você poderá adicionar a opção `-enforce-network-throttling` no início da operação.

> **Note**
>
> O uso dessa opção afeta a entrada SnapMirror transferências de dados de replicação para o sistema de arquivos. Tenha atenção em como configura as opções de replicação do seu sistema de arquivos, pois você não pode visualizá-las depois de configurá-las.

Para controlar a utilização de uma movimentação de volume

1. O controle de utilização usa o controle global de replicação. Para definir o acelerador de replicação global, use o seguinte comando no ONTAP CLI.

   ```
   ::> options -option-name replication.throttle.enable on
   ```

2. Especifique a largura de banda total máxima que pode ser usada pela replicação, substituindo a seguinte opção:

   - `kbs_throttle`com a taxa de transferência máxima desejada para usar em qualquer replicação (inclusive SnapMirror e movimentos de volume), em quilobytes por segundo.

   ```
   ::> options -option-name replication.throttle.incoming.max_kbs kbs_throttle
   ::> options -option-name replication.throttle.outgoing.max_kbs kbs_throttle
   ```

Monitoramento de volumes

Você pode ver os volumes que estão atualmente em seu sistema de arquivos usando o FSx console da Amazon, o AWS CLI, e a FSx API da Amazon SDKs e.

Para monitorar os volumes no sistema de arquivos:

- Como usar o console: escolha um sistema de arquivos para visualizar a página de detalhes dos Sistemas de arquivos. Escolha a guia Volumes para listar todos os volumes no sistema de arquivos e selecione o que deseja visualizar.

- Usando a CLI ou a API — Use o comando describe-volumes da CLI ou a operação da API. DescribeVolumes

```
$ aws fsx describe-volumes
{
    "Volumes": [
        {
            "CreationTime": "2024-03-04T20:17:44+00:00",
            "FileSystemId": "fs-abcdef0123a0bb087",
            "Lifecycle": "CREATED",
            "Name": "SVM8_ext_root",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
                "JunctionPath": "/",
                "SecurityStyle": "NTFS",
                "SizeInMegabytes": 1024,
                "StorageEfficiencyEnabled": false,
                "StorageVirtualMachineId": "svm-01234567890abcdef",
                "StorageVirtualMachineRoot": true,
                "TieringPolicy": {
                    "Name": "NONE"
                },
                "UUID": "42ce3de0-da64-11ee-a22d-7f7cdfb8d381",
                "OntapVolumeType": "RW",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
                "VolumeStyle": "FLEXVOL",
                "AggregateConfiguration": {
                    "Aggregates": [
                        "aggr1"
                    ]
                },
                "SizeInBytes": 1073741824
            },
            "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcdef0123a0bb087/fsvol-abcdef0123456789a",
            "VolumeId": "fsvol-abcdef0123456789a",
            "VolumeType": "ONTAP"
        }
    ]
}
```

Como visualizar volumes off-line

Você não pode criar ou excluir backups de volume quando o volume de origem estiver off-line. Você pode usar o `volume show` ONTAP Comando CLI para determinar o status atual de um volume.

```
volume show -vserver svm-name
```

Para obter informações sobre como acessar o ONTAP CLI em seu sistema de arquivos, consulte. Usar o NetApp ONTAP CLI

```
FsxIdabc12345::> volume show -vserver vs1
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
vs1       vol1         aggr1        online     RW          2GB      1.9GB    5%
vs1       vol1_dr      aggr0_dp     online     DP        200GB    160.0GB   20%
vs1       vol2         aggr0        online     RW        150GB    110.3GB   26%
vs1       vol2_dr      aggr0_dp     online     DP        150GB    110.3GB   26%
vs1       vol3         aggr1        online     RW        150GB    120.0GB   20%
vs1       vol3_dr      aggr1_dp     online     DP        150GB    120.0GB   20%
vs1       vol4         aggr1        online     RW        200GB    159.8GB   20%
7 entries were displayed.
```

Para colocar um volume off-line novamente on-line, use o `volume online` ONTAP Comando CLI, conforme mostrado no exemplo a seguir. Se existir apenas um SVM (Vserver), você não precisará especificar o `-vserver` parâmetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Excluir volumes do

Você pode excluir um FSx volume do ONTAP usando o FSx console da Amazon AWS CLI, o e a FSx API da Amazon, além do NetApp Interface de linha de comando (CLI) e API REST do ONTAP.

Antes de excluir um volume, certifique-se de que nenhuma aplicação esteja acessando os dados do volume que deseja excluir.

> **Important**
>
> Você só pode excluir volumes usando o FSx console, a API ou a CLI da Amazon se o volume tiver os FSx backups da Amazon habilitados.

Fazendo um backup final do volume

Ao excluir um volume usando o FSx console da Amazon, você tem a opção de fazer um backup final do volume. Como prática recomendada, recomendamos que você opte por fazer um backup final. Se achar que não precisa dele após um determinado período, poderá excluir esse e outros backups de volume criados manualmente. Quando você exclui um volume usando o comando `delete-volume` CLI, a Amazon FSx faz um backup final por padrão.

Para obter mais informações sobre backups de volume, consulteProteger seus dados com backups de volume.

Excluir um volume (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Sistemas de arquivos e o sistema de arquivos do ONTAP do qual deseja excluir um volume.
3. Escolha a guia Volumes.
4. Escolha o volume que deseja excluir.
5. Em Ações, escolha Excluir volume.
6. (SnapLock Enterprise somente volumes) Para Bypass SnapLock Enterprise Retention, escolha Sim.
7. Na caixa de diálogo de confirmação, em Criar backup final, há duas opções:
   - Escolha Sim para fazer um backup final do volume. O nome do backup final é exibido.
   - Escolha Não se não quiser um backup final do volume. Você deverá aceitar que, após a exclusão do volume, os backups automáticos não estarão mais disponíveis.
8. Confirme a exclusão do volume inserindo excluir no campo Confirmar exclusão.
9. Escolha Excluir volumes.

Excluir um volume (CLI)

- Para excluir um volume FSx for ONTAP, use o comando da CLI delete-volume (ou a operação de API DeleteVolumeequivalente), conforme mostrado no exemplo a seguir.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Excluindo SnapLock volumes

Esta seção explica como excluir um SnapLock volume.

Você pode excluir um SnapLock Volume de conformidade se os períodos de retenção de todos os arquivos de gravação única e leitura (WORM) contidos nele expirarem.

> **Note**
>
> Quando você fecha um Conta da AWS que contém SnapLock Enterprise or Compliance volumes AWS e, FSx para o ONTAP, suspenda sua conta por 90 dias, deixando seus dados intactos. Se você não reabrir sua conta durante esses 90 dias, AWS excluirá seus dados, incluindo dados em SnapLock volumes, independentemente de suas configurações de retenção.

Você pode excluir um SnapLock Volume corporativo a qualquer momento, se você tiver as permissões necessárias. Para excluir um SnapLock Volume corporativo usando o ONTAP CLI, você deve ter a `fsxadmin` função. Para obter mais informações, consulte Perfis e usuários de administrador do sistema de arquivos.

Para excluir um SnapLock Volume corporativo que contém dados WORM com uma política de retenção ativa usando o FSx console da Amazon, a CLI ou a API da FSx Amazon, você deve ter `fsx:BypassSnapLockEnterpriseRetention` a permissão do IAM.

> **Warning**
>
> O período mínimo de retenção para um SnapLock o volume do registro de auditoria é de seis meses. Até que esse período de retenção expire, você não poderá excluir o SnapLock volume de log de auditoria, a máquina virtual de armazenamento (SVM) ou o sistema de arquivos associado à SVM, mesmo que o volume tenha sido criado no SnapLock Modo

empresarial. Para obter mais informações, consulte SnapLock volumes de registros de auditoria.

Como criar um LUN de iSCSI

Esse processo descreve como criar um LUN iSCSI em um sistema de arquivos Amazon FSx for NetApp ONTAP usando o NetApp ONTAP Comando CLIlun create. Para obter mais informações, consulte lun createno NetApp ONTAP Centro de documentação.

> **Note**
>
> O protocolo iSCSI não é compatível com sistemas de arquivos com mais de seis pares de HA.

Esse processo pressupõe que você já tenha um volume criado em seu sistema de arquivos. Para obter mais informações, consulte Como criar volumes.

1. Para acessar o ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.
2. Crie um LUN usando o lun create NetApp CLI comando, substituindo os seguintes valores:

   - ***`svm_name`***: o nome da máquina virtual de armazenamento (SVM) que fornece o destino iSCSI. O host usa esse valor para acessar o LUN.
   - ***`vol_name`***: o nome do volume que hospeda o LUN.
   - ***`lun_name`***: o nome que você quer atribuir ao LUN.
   - ***`size`***: o tamanho, em bytes, do LUN. O tamanho máximo do LUN que você pode criar é 128 TB.

> **Note**
>
> Recomendamos que você use um volume pelo menos 5% maior do que o tamanho do LUN. Essa margem deixa espaço para snapshots de volume.

- ***ostype***: o sistema operacional do host, `windows_2008` ou `linux`. Use `windows_2008` para todas as versões do Windows, garantindo assim que o LUN tenha um deslocamento de bloco adequado para o sistema operacional e otimize a performance.

> **Note**
>
> Recomendamos ativar a alocação de espaço no LUN. Com a alocação de espaço habilitada, o ONTAP pode informar o host quando o LUN está sem capacidade e reivindicar espaço à medida que você exclui dados do LUN.

Para obter mais informações, consulte a `lun create`documentação do NetApp ONTAP CLI.

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
ostype ostype -space-allocation enabled
```

```
Created a LUN of size 10g (10737418240)
```

3. Confirme se o LUN foi criado, está on-line e foi mapeado.

```
> lun show
```

O sistema responde com a seguinte saída:

```
Vserver   Path                            State   Mapped   Type         Size
--------- ------------------------------- ------- -------- ------------ --------
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

Próximas etapas

Agora que você criou um LUN de iSCSI, a próxima etapa no processo de usá-lo como armazenamento em blocos é mapear o LUN para um `igroup`. Para ter mais informações, consulte Provisionamento de iSCSI para Linux ou Provisionamento de iSCSI para Windows.

Otimizando o desempenho com as janelas de FSx manutenção da Amazon

Como um serviço totalmente gerenciado, o FSx for ONTAP realiza regularmente manutenção e atualizações em seu sistema de arquivos. Essa manutenção não afeta a maioria das workloads. Para cargas de trabalho que são sensíveis ao desempenho, em raras ocasiões você pode notar um impacto breve (<60 segundos) no desempenho quando a manutenção está ocorrendo; a Amazon FSx permite que você use a janela de manutenção para controlar quando qualquer atividade potencial de manutenção ocorre.

A aplicação de patches ocorre com pouca frequência, normalmente uma vez a cada várias semanas. Quando há a aplicação de patch, cada servidor de arquivos do sistema de arquivos é corrigido um por vez, e a correção de cada servidor de arquivos normalmente leva até uma hora. Antes da aplicação de patch em qualquer servidor de arquivos em um par de HA, seu sistema de arquivos alterna automaticamente para o parceiro de HA dos servidores de arquivos, o que pode resultar em uma breve pausa de E/S (menos de 60 segundos) para qualquer E/S direcionada a esse par de HA. Seu sistema de arquivos então retornará, o que pode resultar em outra breve pausa de E/S (menos de 60 segundos). Você escolhe o horário inicial da janela de manutenção durante a criação do sistema de arquivos. Se você não escolher uma janela, o sistema atribuirá uma automaticamente.

> **Important**
>
> Para garantir que seu sistema de arquivos possa ser corrigido com sucesso, FSx o ONTAP colocará on-line todos os volumes off-line durante o processo de correção. Quaisquer volumes que a Amazon FSx trouxer novamente on-line não estarão acessíveis aos clientes.

FSx for ONTAP permite que você ajuste sua janela de manutenção conforme necessário para acomodar sua carga de trabalho e requisitos operacionais. É possível mover a janela de manutenção com a frequência necessária, desde que uma janela de manutenção ocorra no mínimo uma vez a cada 14 dias. Se um patch for lançado e uma janela de manutenção não ocorrer dentro de 14 dias,

FSx o ONTAP continuará com a manutenção no sistema de arquivos para garantir sua segurança e confiabilidade.

> **Note**
>
> Para garantir a integridade dos dados durante a atividade de manutenção, o FSx for ONTAP fecha todos os bloqueios oportunistas e conclui todas as operações de gravação pendentes nos volumes de armazenamento subjacentes que estão hospedando seu sistema de arquivos antes do início da manutenção.

Você pode usar o Amazon FSx Management Console AWS CLI, a AWS API ou um dos AWS SDKs para alterar a janela de manutenção dos seus sistemas de arquivos.

Alterar a janela de manutenção semanal (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Escolha Sistemas de arquivos na coluna de navegação à esquerda.
3. Escolha o sistema de arquivos do qual deseja alterar a janela de manutenção semanal. A página de detalhes Resumo do sistema de arquivos é exibida.
4. Escolha Administração para exibir o painel Configurações de administração do sistema de arquivos.
5. Escolha Atualizar para exibir a janela Alterar janela de manutenção.
6. Insira o novo dia e horário que você deseja para o início da janela de manutenção semanal.
7. Escolha Salvar para salvar as alterações. O novo horário de início da manutenção é exibido no painel Configurações de administração do sistema de arquivos.

Para alterar a janela de manutenção semanal usando o comando update-file-systemCLI, consulte. Atualizar um sistema de arquivos (CLI)

Como gerenciar a capacidade de throughput

FSx for ONTAP configura a capacidade de taxa de transferência quando você cria o sistema de arquivos. Você pode modificar a capacidade de throughput do sistema de arquivos a qualquer momento. Lembre-se de que seu sistema de arquivos requer uma configuração específica para atingir a quantidade máxima de capacidade de throughput. Por exemplo, para provisionar 4% GBps

da capacidade de taxa de transferência para um sistema de arquivos de primeira geração, seu sistema de arquivos requer uma configuração com um mínimo de 5.120 GiB de capacidade de armazenamento SSD e 160.000 SSD IOPS. Para obter mais informações, consulte Impacto da capacidade de throughput na performance.

A capacidade de throughput é um fator que determina a velocidade com que o servidor de arquivos que hospeda o sistema de arquivos pode fornecer os dados de arquivos. Níveis mais altos de capacidade de throughput vêm com níveis mais altos de rede, operações de E/S de leitura de disco por segundo (IOPS) e capacidade de armazenamento de dados em cache no servidor de arquivos. Para obter mais informações, consulte Performance.

Quando você modifica a capacidade de taxa de transferência do seu sistema de arquivos, a Amazon FSx troca o servidor de arquivos que está alimentando seu sistema de arquivos. Os sistemas de arquivos single-AZ e multi-AZ passam por um failover e um failback automáticos durante esse processo, que normalmente leva alguns minutos para ser concluído. Os processos de failover e failback são transparentes para os clientes NFS (Network File Sharing), SMB (Server Message Block) e iSCSI (Internet Small Computer Systems Interface), permitindo que suas workloads continuem em execução sem interrupção ou intervenção manual. Você receberá uma cobrança pela nova quantidade de capacidade de throughput quando ela estiver disponível para o seu sistema de arquivos.

> **Note**
>
> Para garantir a integridade dos dados durante a atividade de manutenção, o FSx for ONTAP fecha todos os bloqueios oportunistas e conclui todas as operações de gravação pendentes nos volumes de armazenamento subjacentes que estão hospedando seu sistema de arquivos antes do início da manutenção. Durante uma janela de manutenção programada do sistema de arquivos, as modificações do sistema (como as modificações na capacidade de throughput) podem atrasar. A manutenção do sistema pode fazer com que essas alterações fiquem na fila até que sejam processadas. Para obter mais informações, consulte the section called “Atualizar janelas de manutenção”.

Tópicos

- Quando modificar a capacidade de throughput
- Como as solicitações simultâneas são processadas
- Atualizar a capacidade de throughput

- Como monitorar as alterações na capacidade de throughput

Quando modificar a capacidade de throughput

A Amazon FSx se integra à Amazon CloudWatch, o que ajuda você a monitorar os níveis contínuos de uso da taxa de transferência do seu sistema de arquivos. A performance do throughput e das IOPS que você pode direcionar por meio do sistema de arquivos dependem das características específicas da workload, além da capacidade de throughput do sistema de arquivos. Como regra, você deve provisionar capacidade de throughput suficiente para suportar o throughput de leitura da sua workload mais o dobro do throughput de gravação da workload. Você pode usar CloudWatch métricas para determinar quais dessas dimensões devem ser alteradas para melhorar o desempenho. Para obter mais informações, consulte the section called “Monitoramento no FSx console da Amazon”.

Como as solicitações simultâneas são processadas

Para sistemas de arquivos de primeira geração, você pode solicitar uma atualização da capacidade de throughput pouco antes do início do fluxo de trabalho de atualização da capacidade de armazenamento SSD e das IOPS provisionadas ou enquanto ele estiver em andamento. A sequência de como a Amazon FSx lida com as duas solicitações é a seguinte:

- Se você enviar uma SSD/IOPS update and throughput capacity update at the same time, both requests are accepted. The SSD/IOPS atualização, será priorizada antes da atualização da capacidade de taxa de transferência.
- Se você enviar uma atualização da capacidade de taxa de transferência enquanto uma SSD/IOPS update is in progress, the throughput capacity update request is accepted and queued to occur after the SSD/IOPS update. The throughput capacity update starts after SSD/IOPS é atualizada (novos valores estão disponíveis) e durante a etapa de otimização. Normalmente, isso demora menos de dez minutos.
- Se você enviar uma solicitação SSD/IOPS update while a throughput capacity update is in progress, the SSD/IOPS de atualização de armazenamento, ela será aceita e colocada na fila para começar após a conclusão da atualização da capacidade de taxa de transferência (nova capacidade de taxa de transferência está disponível). Normalmente, isso demora 20 minutos.

Considere os seguintes pontos ao solicitar uma atualização da capacidade de throughput para sistemas de arquivos de segunda geração:

- Você deve aguardar no mínimo 6 horas entre a atualização da capacidade de throughput dos sistemas de arquivos de segunda geração.
- O período de espera da capacidade de throughput é compartilhado com o escalonamento de SSD/IOPS.
- O escalonamento da capacidade de throughput e o escalonamento de SSD/IOPS não podem ser feitos simultaneamente ou colocados em fila enquanto algum deles estiver em andamento.
- Você não pode adicionar pares de alta disponibilidade (HA) em conjunto com ou durante o escalonamento da capacidade de taxa de transferência ou escalabilidade e escalabilidade da capacidade de taxa SSD/IOPS scaling are in progress. However, adding HA pairs doesn't share a cooldown with SSD/IOPS de transferência. Para obter mais informações, consulte Adicionar pares de alta disponibilidade (HA).

Para obter mais informações sobre atualizações de armazenamento SSD e de IOPS provisionadas, consulte Como gerenciar a capacidade de armazenamento.

Atualizar a capacidade de throughput

Você pode modificar a capacidade de taxa de transferência de um sistema de arquivos usando o FSx console da Amazon, o AWS Command Line Interface (AWS CLI) ou a FSx API da Amazon.

> **Note**
>
> Você deve aguardar no mínimo 6 horas entre a atualização da capacidade de throughput dos sistemas de arquivos de segunda geração.

Modificar a capacidade de throughput de um sistema de arquivos (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do ONTAP para o qual você deseja aumentar a capacidade de throughput.
3. Em Ações, escolha Atualizar capacidade de throughput. Como alternativa, no painel Resumo, escolha Atualizar ao lado da Capacidade de throughput do sistema de arquivos.
4. Escolha o novo valor para Capacidade de throughput na lista.
5. Escolha Atualizar para iniciar a atualização da capacidade de throughput.

6. Você pode monitorar o progresso da atualização na página de detalhes dos Sistemas de arquivos, na guia Atualizações.

   Você pode monitorar o progresso da atualização usando o FSx console da Amazon AWS CLI, o e a API. Para obter mais informações, consulte Como monitorar as alterações na capacidade de throughput.

Modificar a capacidade de throughput de um sistema de arquivos (CLI)

Para modificar a capacidade de taxa de transferência de um sistema de arquivos, use o AWS CLI comando update-file-system. Defina os seguintes parâmetros:

- `--file-system-id` para o ID do sistema de arquivos que você está atualizando.
- `ThroughputCapacity` para o valor desejado para o qual atualizar o sistema de arquivos.

Você pode monitorar o progresso da atualização usando o FSx console da Amazon AWS CLI, o e a API. Para obter mais informações, consulte Como monitorar as alterações na capacidade de throughput.

Como monitorar as alterações na capacidade de throughput

Você pode monitorar o progresso de uma modificação da capacidade de transferência usando o FSx console da Amazon, a API e o. AWS CLI

Como monitorar as alterações na capacidade de throughput no console

Na guia Atualizações, na janela Detalhes do sistema de arquivos, você pode visualizar as dez ações de atualização mais recentes para cada tipo de ação de atualização.

Nas ações de atualização da capacidade de throughput, é possível visualizar as informações apresentadas a seguir.

Tipo de atualização

Os tipos compatíveis são Capacidade de throughput, Capacidade de armazenamento e Otimização de armazenamento.

Target value (Valor de destino)

O valor desejado para o qual alterar a capacidade de throughput do sistema de arquivos.

Status

O status atual da atualização. Para atualizações de capacidade de throughput, os valores possíveis são:

- Pendente — a Amazon FSx recebeu a solicitação de atualização, mas ainda não começou a processá-la.
- Em andamento — a Amazon FSx está processando a solicitação de atualização.
- Concluído: a atualização da capacidade de throughput foi concluída com êxito.
- Com falha: a atualização da capacidade de throughput falhou. Escolha o ponto de interrogação (?) para ver os detalhes sobre o motivo da falha na atualização do throughput.

Horário da solicitação

A hora em que a Amazon FSx recebeu a solicitação de atualização.

Monitorando mudanças com a API AWS CLI e

Você pode visualizar e monitorar as solicitações de modificação da capacidade da taxa de transferência do sistema de arquivos usando o comando describe-file-systemsCLI e DescribeFileSystemsa ação da API. A matriz `AdministrativeActions` lista as dez ações de atualização mais recentes para cada tipo de ação administrativa. Ao modificar a capacidade de throughput de um sistema de arquivos, é gerada uma ação administrativa `FILE_SYSTEM_UPDATE`.

O exemplo apresentado a seguir mostra um trecho da resposta de um comando `describe-file-systems` da CLI. O sistema de arquivos tem uma capacidade de taxa de transferência de 128 MBps e uma capacidade de taxa de transferência alvo de 256. MBps

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
```

```
          }
        }
    }
]
```

Quando a Amazon FSx processa a ação com sucesso, o status muda para`COMPLETED`. A nova capacidade de throughput fica então disponível para o sistema de arquivos e é mostrada na propriedade `ThroughputCapacity`. Isso é mostrado no trecho de resposta a seguir de um comando describe-file-systems da CLI.

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Se a modificação da capacidade de throughput apresentar falhas, o status será alterado para `FAILED` e a propriedade `FailureDetails` fornecerá informações sobre a falha.

Como gerenciar compartilhamentos de SMB

Para gerenciar compartilhamentos de arquivos SMB em seu sistema de FSx arquivos da Amazon, você pode usar a GUI de pastas compartilhadas do Microsoft Windows. A GUI de pastas compartilhadas fornece um local central para gerenciar todas as pastas compartilhadas de sua máquina virtual de armazenamento (SVM). Os procedimentos a seguir detalham como criar, atualizar e remover compartilhamentos de arquivos.

> **Note**
>
> Você também pode gerenciar compartilhamentos de arquivos SMB usando o NetApp System Manager. Para obter mais informações, consulte O uso do NetApp Gerenciador de sistemas com BlueXP.

Para conectar pastas compartilhadas ao seu sistema de FSx arquivos da Amazon

1. Inicie sua EC2 instância da Amazon e conecte-a ao Microsoft Active Directory ao qual seu sistema de FSx arquivos da Amazon está associado. Para fazer isso, escolha um dos seguintes procedimentos no Guia de administração do AWS Directory Service :
   - Junte-se perfeitamente a uma instância do Windows EC2
   - Associar manualmente uma instância do Windows
2. Conecte-se a uma instância como usuário membro do grupo de administradores do sistema de arquivos. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia EC2 do usuário da Amazon.
3. Abra o menu Iniciar e execute fsmgmt.msc usando Executar como administrador. Essa ação abre a ferramenta de pastas compartilhadas da GUI.
4. Em Ação, escolha Conectar a outro computador.
5. Em Outro computador, insira o nome DNS da sua máquina virtual de armazenamento (SVM), por exemplo, **`netbios_name.corp.example.com`**.

   Para encontrar o nome DNS da sua SVM no FSx console da Amazon, escolha Máquinas virtuais de armazenamento, escolha sua SVM e, em seguida, role para baixo até Endpoints até encontrar o nome DNS do SMB. Você também pode obter o nome DNS na resposta da operação da DescribeStorageVirtualMachinesAPI.
6. Escolha OK. Em seguida, uma entrada para o sistema de FSx arquivos da Amazon aparece na lista da ferramenta de pastas compartilhadas.

Agora que as pastas compartilhadas estão conectadas ao seu sistema de FSx arquivos da Amazon, você pode gerenciar os compartilhamentos de arquivos do Windows no sistema de arquivos com as seguintes ações:

> **Note**
>
> Recomendamos que você localize seus compartilhamentos SMB em um volume diferente do volume raiz.

- Crie um novo compartilhamento de arquivos — Na ferramenta Pastas compartilhadas, escolha Compartilhamentos no painel esquerdo para ver os compartilhamentos ativos do seu sistema de FSx arquivos da Amazon. Os volumes são mostrados montados no caminho escolhido durante a criação do volume. Escolha Novo compartilhamento e conclua o assistente de criação de uma pasta compartilhada.

  Você precisa criar a pasta local antes de criar o novo compartilhamento de arquivos. Você pode fazer isso da seguinte maneira:

  - Usando a ferramenta Pastas compartilhadas: escolha Procurar ao especificar um caminho de pasta local, escolha Criar nova pasta para criar a pasta local.
  - Como usar a linha de comando:

    ```
    New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
    $volume_path\MyNewFolder
    ```

- Modificar um compartilhamento de arquivos: na ferramenta Pastas compartilhadas, abra o menu de contexto (clique com o botão direito do mouse) do compartilhamento de arquivos a ser modificado no painel direito e selecione Propriedades. Modifique as propriedades e escolha OK.
- Remover um compartilhamento de arquivos: na ferramenta Pastas compartilhadas, abra o menu de contexto (clique com o botão direito do mouse) do compartilhamento de arquivos a ser removido no painel direito e escolha Interromper o compartilhamento.

  > **Note**
  >
  > A remoção de compartilhamentos de arquivos da GUI só é possível se você estiver conectado ao fsmgmt.msc usando o nome DNS do sistema de arquivos da Amazon. FSx Se você se conectou usando o endereço IP ou o nome do alias DNS do sistema de arquivos, a opção Interromper o compartilhamento não funcionará e o compartilhamento de arquivos não será removido.

Gerenciando FSx recursos do ONTAP usando NetApp aplicações

Além da AWS API AWS Management Console, AWS CLI, e SDKs, você também pode usar esses NetApp ferramentas e aplicativos de gerenciamento para gerenciar seus FSx recursos do ONTAP:

Tópicos

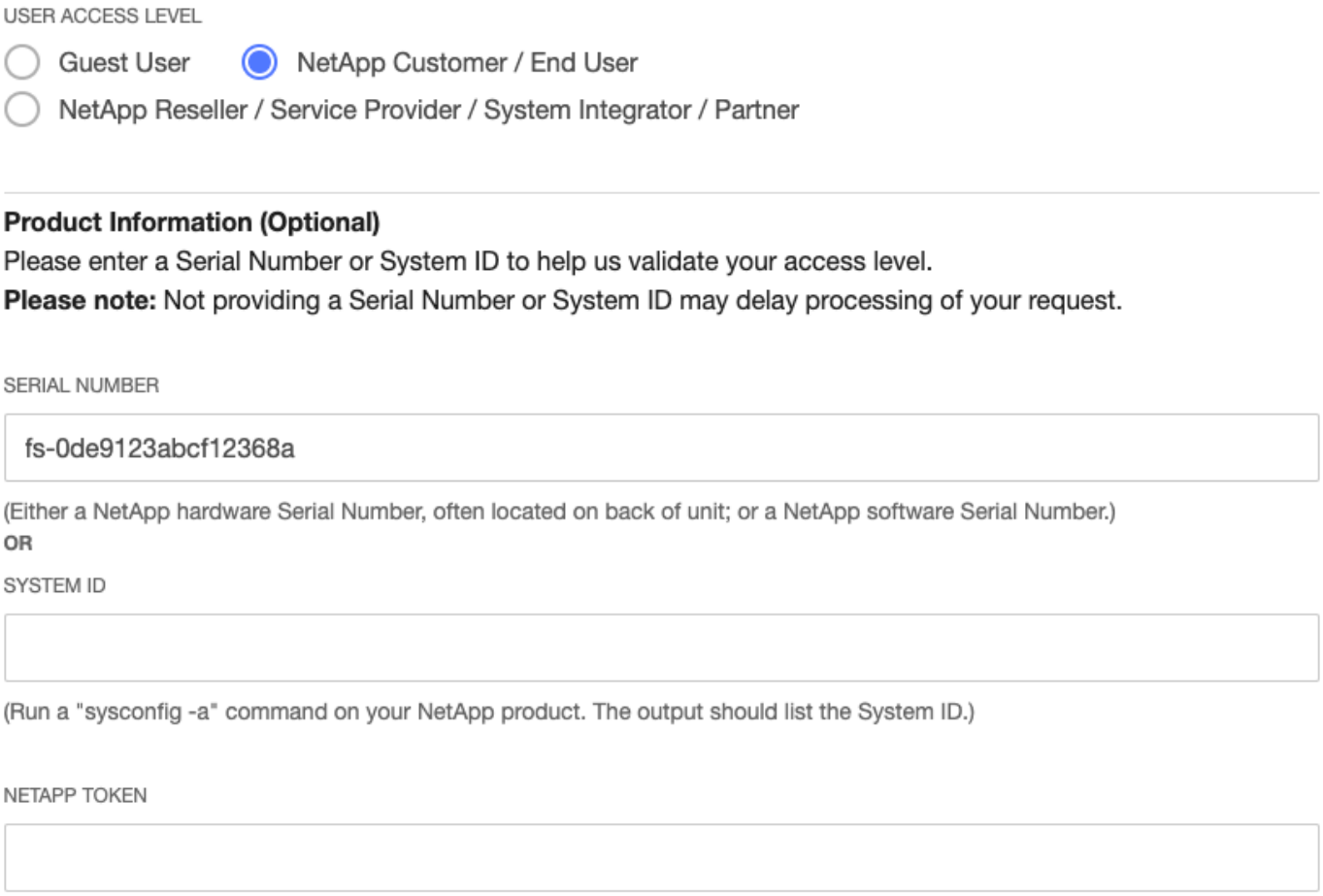
- Inscrevendo-se para um NetApp conta
- O uso do NetApp BlueXP
- Usar o NetApp ONTAP CLI
- Usar o ONTAP API REST

> **Important**
>
> A Amazon sincroniza FSx periodicamente com ONTAP para garantir a consistência. Se você criar ou modificar volumes usando NetApp aplicativos, pode levar alguns minutos para que essas alterações sejam refletidas na AWS Management Console, AWS CLI, API SDKs e.

Inscrevendo-se para um NetApp conta

Para baixar alguns NetApp software, como BlueXP, SnapCenter, e o ONTAP Conector antivírus, você precisa ter um NetApp conta. Para se inscrever em um NetApp conta, execute as seguintes etapas:

1. Vá para o NetAppPágina de registro do usuário e cadastre-se para uma nova NetApp conta de usuário.
2. Preencha os formulários com suas informações. Certifique-se de selecionar o NetApp Nível de acesso do cliente/usuário final. No campo NÚMERO DE SÉRIE, copie e cole a ID do sistema de arquivos do seu sistema FSx de arquivos ONTAP. Veja o exemplo a seguir:



O que esperar após o cadastro

Clientes com clientes existentes NetApp os produtos terão sua conta NSS nivelada até o nível de acesso ao nível do cliente em um dia útil. Clientes novos em NetApp serão integrados usando práticas comerciais padrão, além de ter sua conta NSS nivelada até o nível de acesso ao nível de cliente. Fornecer o ID do sistema de arquivos ajudará a acelerar esse processo. Você pode verificar o status da sua conta NSS fazendo login em mysupport.netapp.com e navegando até a página Welcome. O nível de acesso da sua conta deve ser Customer Access.

O uso do NetApp BlueXP

NetApp O BlueXP é um plano de controle unificado que simplifica as experiências de gerenciamento de serviços de armazenamento e dados em ambientes locais e na nuvem. O BlueXP fornece uma interface de usuário centralizada para gerenciar, monitorar e automatizar as implantações do ONTAP

no local e no local. AWS Para obter mais informações, consulte a documentação do NetApp BlueXP e a documentação do NetApp BlueXP for FSx Amazon NetApp for ONTAP.

> **Note**
>
> NetApp BlueXP não é compatível com sistemas de arquivos de segunda geração com mais de um par de alta disponibilidade (HA).

O uso do NetApp Gerenciador de sistemas com BlueXP

Você pode gerenciar seus sistemas de arquivos Amazon FSx for NetApp ONTAP usando o System Manager diretamente do BlueXP. BlueXP permite que você use a mesma interface do System Manager que você está acostumado a usar, para que você possa gerenciar sua infraestrutura híbrida de várias nuvens a partir de um único plano de controle. Você também tem acesso às outras funcionalidades do BlueXP. Para obter mais informações, consulte o tópico Integração do System Manager com o BlueXP no NetApp Documentação do ONTAP.

> **Note**
>
> NetApp O System Manager não é compatível com sistemas de arquivos de segunda geração com mais de um par de HA.

Usar o NetApp ONTAP CLI

Você pode gerenciar seus recursos do Amazon FSx for NetApp ONTAP usando o NetApp ONTAP CLI. Você pode gerenciar recursos no sistema de arquivos (análogo ao NetApp ONTAP (cluster) e no nível do SVM.

Gerenciando sistemas de arquivos com o ONTAP CLI

Você pode correr ONTAP Comandos CLI em seu sistema de arquivos FSx for ONTAP, semelhantes à execução deles em um NetApp ONTAP cluster. Você acessa o ONTAP CLI em seu sistema de arquivos estabelecendo uma conexão shell segura (SSH) com o endpoint de gerenciamento do sistema de arquivos e fazendo login com o nome de usuário e a `fsxadmin` senha. Você tem a opção de definir a `fsxadmin` senha ao criar um sistema de arquivos usando o fluxo de criação personalizado ou usando AWS CLI o. Se você criou o sistema de arquivos usando a opção Criação

rápida, a `fsxadmin` senha não foi definida, então você precisará definir uma para fazer login no ONTAP CLI. Para obter mais informações sobre como definir a senha do sistema de `fsxadmin` arquivos, consulteAtualizar sistemas de arquivos. Você pode encontrar o nome DNS e o endereço IP do endpoint de gerenciamento do seu sistema de arquivos no FSx console da Amazon, na guia Administração da página de detalhes do FSx sistema de arquivos do ONTAP.

Para se conectar ao endpoint de gerenciamento do sistema de arquivos com SSH, primeiro faça login em uma EC2 instância na mesma VPC do sistema de arquivos do FSx ONTAP. Depois de fazer login na EC2 instância, use o `fsxadmin` usuário e a senha para fazer SSH no endereço IP ou nome DNS do endpoint de gerenciamento do sistema de arquivos, como nos exemplos a seguir.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

O comando de SSH com valores de exemplo:

```
ec2user $ ssh fsxadmin@198.51.100.0
```

O comando SSH usando o nome DNS do endpoint de gerenciamento:

```
ec2user $ ssh fsxadmin@file-system-management-endpoint-dns-name
```

O comando de SSH usando um nome de DNS de exemplo:

```
ec2user $ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin_password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Escopo do ONTAP Comandos CLI disponíveis para **`fsxadmin`**

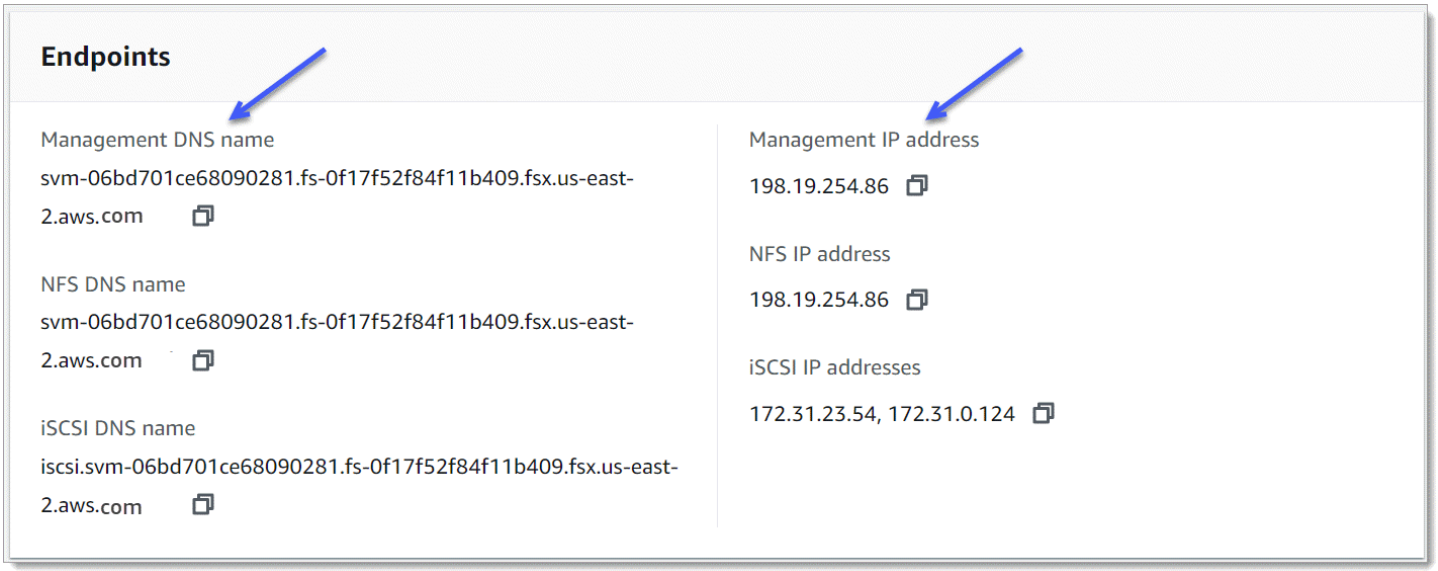
A visão administrativa `fsxadmin` do sistema de arquivos está no nível do sistema de arquivos, que inclui todos SVMs os volumes do sistema de arquivos. O `fsxadmin` papel desempenha o papel do ONTAP administrador do cluster. Como os sistemas de arquivos Amazon FSx for NetApp ONTAP são totalmente gerenciados, a `fsxadmin` função pode executar um subconjunto dos disponíveis ONTAP Comandos da CLI.

Para ver uma lista dos comandos que `fsxadmin` podem ser executados, use o seguinte `security login role show` ONTAP Comando da CLI:

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
           Role          Command/                                    Access
Vserver    Name          Directory                             Query Level
---------- ------------- --------- ----------------------------------- --------
FsxId0abcdef123456789
           fsxadmin      application                                   all
                         cluster application-record                    all
                         cluster date show                             readonly
                         cluster ha modify                             readonly
                         cluster ha show                               readonly
                         cluster identity modify                       readonly
                         cluster identity show                         readonly
                         cluster log-forwarding           -port !55555 all
                         cluster modify                                readonly
                         cluster peer                                  all
                         cluster show                                  readonly
                         cluster statistics show                       readonly
                         cluster time-service ntp server create        readonly
                         cluster time-service ntp server delete        readonly
                         cluster time-service ntp server modify        readonly
                         cluster time-service ntp server show          readonly
                         debug network tcpdump       -ipspace !Cluster all
                         debug san lun                                 all
                         df         -vserver !FsxId* -vserver !Cluster readonly
                         echo                                          all
                         event catalog show                            readonly
                         event config                                  all
.
.
.
378 entries were displayed.
```

Gerenciando SVMs com o ONTAP CLI

Você pode acessar o ONTAP CLI em sua SVM estabelecendo uma conexão de shell segura (SSH) com o endpoint de gerenciamento da SVM usando o nome de usuário e a senha. `vsadmin` Você pode encontrar o nome DNS e o endereço IP do endpoint de gerenciamento do SVM no FSx console da Amazon, no painel Endpoints da página de detalhes das máquinas virtuais de armazenamento, mostrada no gráfico a seguir.



Para se conectar ao endpoint de gerenciamento do SVM com SSH, você pode usar o `vsadmin` nome de usuário e a senha. Se não tiver definido uma senha para o usuário `vsadmin` quando a SVM foi criada, você poderá definir a senha de `vsadmin` a qualquer momento. Para obter mais informações, consulte Atualizar máquinas virtuais de armazenamento (SVM). Você pode efetuar SSH na SVM por meio de um cliente que esteja na mesma VPC do sistema de arquivos, usando o endereço IP ou o nome DNS do endpoint de gerenciamento.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

O comando com exemplo de valores:

```
ssh vsadmin@198.51.100.10
```

O comando SSH usando o nome DNS do endpoint de gerenciamento:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

O comando de SSH usando um nome de DNS de exemplo:

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
```

```
FsxId0abcdef123456789::>
```

O Amazon FSx for NetApp ONTAP oferece suporte ao NetApp ONTAP Comandos da CLI.

Para uma referência completa de NetApp ONTAP Comandos CLI, consulte Comandos ONTAP: Referência da página de manual.

Usar o ONTAP API REST

Ao acessar seu sistema de arquivos FSx for ONTAP usando o ONTAP Com a API REST usando `fsxadmin` as credenciais, faça o seguinte:

- Desabilite a validação TLS.

  Ou

- Confie nas autoridades de AWS certificação (CAs) — O pacote de certificados para o CAs em cada região pode ser encontrado no seguinte URLs endereço:
  - https://fsx-aws-certificates.s3.amazonaws.com/bundle- *`aws-region`* .pem para público Regiões da AWS
  - https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle- *`aws-region`* .pem para regiões AWS GovCloud
  - https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle- .pem para regiões da China *`aws-region`* AWS

Para uma referência completa de NetApp ONTAP Comandos da API REST, consulte o NetApp ONTAP Referência on-line da API REST.

Marcação de recursos da Amazon FSx

Para ajudá-lo a gerenciar seus sistemas de arquivos e outros FSx recursos da Amazon, você pode atribuir seus próprios metadados a cada recurso na forma de tags. Com as tags, você pode categorizar seus AWS recursos de maneiras diferentes, por exemplo, por finalidade, proprietário ou ambiente. Essa categorização é útil quando você tem muitos recursos do mesmo tipo. Você pode identificar rapidamente um recurso específico com base nas tags atribuídas a ele. Este tópico descreve tags e mostra a você como criá-las.

Tópicos

- Conceitos Básicos de Tags

- Marcando seus Recursos
- Copiar tags para backups
- Restrições de tags
- Permissões e marcação de tags

Conceitos Básicos de Tags

Uma tag é um rótulo que você atribui a um AWS recurso. Cada tag consiste em duas partes que você define:

- Uma chave de tag (por exemplo `CostCenter`, `Environment` ou `Project`). Chaves de tag fazem distinção entre maiúsculas e minúsculas.
- Um valor de tag (por exemplo, `111122223333` ou `Production`). Como chaves de tag, os valores das tags diferenciam maiúsculas de minúsculas. Os valores das tags são opcionais.

Você pode usar tags para categorizar seus AWS recursos de maneiras diferentes, como por finalidade, proprietário ou ambiente. Por exemplo, você pode definir um conjunto de tags para os sistemas de FSx arquivos da Amazon da sua conta que ajuda a rastrear o proprietário e o nível de pilha de cada instância.

Recomendamos que você desenvolva um conjunto de chave de tags que atenda suas necessidades para cada tipo de recurso. Usar um conjunto consistente de chaves de tags facilita para você gerenciar seus recursos. É possível pesquisar e filtrar os recursos de acordo com as tags que adicionar. Para obter mais informações sobre como implementar uma estratégia eficaz de marcação de recursos, consulte Como marcar AWS recursos no. Referência geral da AWS

Alguns comportamentos de marcação com tags a serem considerados:

- As tags não têm nenhum significado semântico para a Amazon FSx e são interpretadas estritamente como uma sequência de caracteres.
- Tags não são automaticamente atribuídas aos recursos.
- É possível editar chaves de tags e valores e é possível remover as tags de um recurso a qualquer momento.
- Você pode definir o valor de uma tag para uma string vazia, mas esse valor não pode ser definido como `null`.

- Ao adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo.
- Se você excluir um recurso, todas as tags do recurso também serão excluídas.
- Se você estiver usando a FSx API da Amazon, o AWS Command Line Interface (AWS CLI) ou um AWS SDK, você pode fazer o seguinte:
  - Você pode usar a ação de API `TagResource` para aplicar tags a recursos existentes.
  - Para algumas ações de criação de recursos, será possível especificar tags para um recurso quando ele for criado. Ao marcar com tags os recursos no momento da criação, você elimina a necessidade de executar scripts personalizados de uso de tags após a criação do recurso.

    Se as tags não puderem ser aplicadas durante a criação do recurso, a Amazon FSx reverte o processo de criação do recurso. Esse comportamento ajuda a garantir que os recursos sejam criados com tags ou, então, não sejam criados, e que nenhum recurso seja deixado sem tags em nenhum momento.

    > **Note**
    >
    > Certas permissões AWS Identity and Access Management (IAM) são necessárias para que os usuários marquem recursos na criação. Para obter mais informações, consulte Conceder permissão para marcar recursos durante a criação.

Marcando seus Recursos

Você pode marcar FSx os recursos da Amazon que existem na sua conta. Se você estiver usando o FSx console da Amazon, poderá aplicar tags aos recursos usando a guia Tags na tela do recurso relevante. Ao criar recursos, você pode aplicar a chave Nome com um valor e aplicar tags de sua escolha ao criar um sistema de arquivos. No entanto, embora o console organize os recursos de acordo com a chave Name, essa chave não tem nenhum significado semântico para o serviço da Amazon FSx .

Para implementar um controle granular sobre os usuários e grupos que podem marcar recursos na criação, você pode aplicar permissões em nível de recurso baseadas em tags em suas políticas do IAM às ações de FSx API da Amazon que oferecem suporte à marcação na criação. Ao usar essas permissões nas suas políticas, você obtém os seguintes benefícios:

- Seus recursos ficam devidamente protegidos desde a criação.

- Como as tags são aplicadas instantaneamente aos seus recursos, todas as permissões em nível de recurso baseadas em tags que controlam o uso de recursos entram imediatamente em vigor.
- Seus recursos podem ser rastreados e relatados com mais precisão.
- É possível obrigar o uso de marcação com tags nos novos recursos e controlar quais chaves e valores de tag são definidos nos seus recursos.

Para controlar quais chaves e valores de tag são definidos em seus recursos existentes, você pode aplicar permissões em nível de recurso às ações de FSx API `TagResource` da `UntagResource` Amazon e às suas políticas do IAM.

Para obter mais informações sobre as permissões necessárias para marcar os FSx recursos da Amazon no momento da criação, consulteConceder permissão para marcar recursos durante a criação.

Para obter mais informações sobre o uso de tags para restringir o acesso aos FSx recursos da Amazon nas políticas do IAM, consulteUsando tags para controlar o acesso aos seus FSx recursos da Amazon.

Para obter informações sobre a aplicação de tags nos seus recursos para fins de faturamento, consulte Usar tags de alocação de custos no Guia do usuário do AWS Billing .

Copiar tags para backups

Ao criar ou atualizar um volume na FSx API da Amazon ou AWS CLI, você pode habilitar `CopyTagsToBackups` a cópia automática de qualquer tag de seus volumes para backups.

> **Note**
>
> Se você especificar tags ao criar um backup iniciado pelo usuário (incluindo a tag de nome ao criar um backup usando o FSx console da Amazon), as tags não serão copiadas do volume, mesmo que você tenha habilitado. `CopyTagsToBackups`

Para obter mais informações sobre backups, consulte Proteger seus dados com backups de volume. Para obter mais informações sobre a habilitação`CopyTagsToBackups`, consulte Para criar um volume (CLI) e Atualizar a configuração de um volume (CLI) no Guia do usuário do Amazon FSx for NetApp ONTAP ou CreateVolumeUpdateVolumena Referência da API Amazon FSx for NetApp ONTAP.

Restrições de tags

As restrições básicas a seguir se aplicam a tags:

- O número máximo de tags por recurso é 50.
- O comprimento máximo da chave da é de 128 caracteres Unicode em UTF-8.
- O comprimento máximo do valor da é de 256 caracteres Unicode em UTF-8.
- Os caracteres permitidos são letras, números e espaços representáveis em UTF-8, além dos seguintes caracteres: `+ - =` (hífen) `. _` (sublinhado) `: / @`.
- Em todos os recursos, cada chave de tag deve ser exclusiva e possuir apenas um valor.
- As chaves e valores das tags diferenciam maiúsculas de minúsculas.
- O `aws:` prefixo está reservado para AWS uso. Não é possível editar nem excluir a chave ou o valor de uma tag se ela tiver uma chave de tag com esse prefixo. As tags com o prefixo `aws:` não contam para as tags por limite de recurso.

Você não pode excluir um recurso unicamente com base em suas tags, portanto, você deve especificar o identificador de recursos. Por exemplo, para excluir um sistema de arquivos marcados com uma chave de tag denominada `DeleteMe`, use a ação `DeleteFileSystem` com o identificador de recursos do sistema de arquivos, como `fs-1234567890abcdef0`.

Quando você marca recursos públicos ou compartilhados, as tags que você atribui ficam disponíveis somente para você Conta da AWS; nenhuma outra Conta da AWS pessoa tem acesso a essas tags. Para o controle de acesso baseado em tags aos recursos compartilhados, cada um Conta da AWS deve atribuir seu próprio conjunto de tags para controlar o acesso ao recurso.

Permissões e marcação de tags

Para obter mais informações sobre as permissões necessárias para marcar os FSx recursos da Amazon no momento da criação, consulteConceder permissão para marcar recursos durante a criação.

Para obter mais informações sobre o uso de tags para restringir o acesso aos FSx recursos da Amazon nas políticas do IAM, consulteUsando tags para controlar o acesso aos seus FSx recursos da Amazon.

Como proteger seus dados

Além de replicar automaticamente os dados do seu sistema de arquivos para garantir alta durabilidade, com a Amazon FSx você também tem as seguintes opções que podem ser usadas para proteger ainda mais seus dados:

- Backups de FSx volume nativos da Amazon que suportam suas necessidades de retenção e conformidade de backup na Amazon FSx.
- Usando AWS Backup para implementar uma estratégia de backup e retenção automatizada e gerenciada centralmente em vários Serviços da AWS.
- Instantâneos que permitem que seus usuários desfaçam facilmente alterações indesejadas em arquivos, restaurando arquivos para versões anteriores.
- Use SnapLock criar volumes de armazenamento de gravação uma vez, leitura múltipla (WORM) para evitar a modificação ou exclusão de arquivos depois de confirmados, por um período de retenção especificado.
- FlexCache os volumes oferecem replicação de dados eficiente em termos de armazenamento, econômica e de alto desempenho para cargas de trabalho com muita leitura, com dados que permanecem praticamente inalterados.
- Use SnapMirror criar uma replicação programada e automática do sistema de arquivos em um segundo sistema de arquivos para proteção de dados e recuperação de desastres.

Tópicos

- Proteger seus dados com backups de volume
- Como proteger seus dados com snapshots
- Protegendo seus dados com a Proteção Autônoma contra Ransomware
- Protegendo seus dados com SnapLock
- Replicando seus dados com FlexCache
- Replicando seus dados usando NetApp SnapMirror

Proteger seus dados com backups de volume

Com FSx o ONTAP, você pode proteger seus dados fazendo backups diários automáticos e backups iniciados pelo usuário dos volumes em seu sistema de arquivos. Criar backups rotineiros para

os volumes é uma prática recomendada que ajuda a apoiar suas necessidades de retenção e conformidade de dados. Você pode restaurar backups de volume em qualquer sistema FSx de arquivos ONTAP existente ao qual você tenha acesso e que esteja no mesmo Região da AWS local em que o backup está armazenado. Trabalhar com FSx os backups da Amazon facilita a criação, a visualização, a restauração e a exclusão de backups de seus volumes.

A Amazon FSx oferece suporte ao backup `OntapVolumeType` de ONTAP volumes com leitura e gravação (RW).

> **Note**
>
> A Amazon FSx não oferece suporte ao backup de volumes de proteção de dados (DP), volumes de espelho de compartilhamento de carga (LSM) ou volumes de destino para e. FlexCache SnapMirror

Tópicos

- Como funcionam os backups
- Requisitos de armazenamento
- Backups automáticos diários
- Backups iniciados pelo usuário
- Copiar tags para backups
- Usando AWS Backup com a Amazon FSx
- Restaurar backups em um novo volume
- Desempenho de backup e restauração
- Fazer o backup de volumes do SnapLock
- Como criar backups iniciados pelo usuário
- Restaurar um backup em um novo volume
- Restaurar um subconjunto de dados
- Monitorar o andamento ao restaurar um backup
- Excluir backups

Como funcionam os backups

Todos os FSx backups da Amazon (backups diários automáticos e backups iniciados pelo usuário) são incrementais, o que significa que eles armazenam apenas as alterações nos dados desde a conclusão do backup anterior. Isso minimiza o tempo necessário para criar um backup e a quantidade de armazenamento usada por cada backup. Os backups incrementais otimizam os custos de armazenamento ao não armazenar dados duplicados. FSx para ONTAP, os backups são por volume, com cada backup contendo somente os dados de um volume específico. Os FSx backups da Amazon são armazenados de forma redundante em várias zonas de disponibilidade para alcançar alta durabilidade.

FSx Os backups da Amazon usam instantâneos — point-in-time imagens somente para leitura dos seus volumes — para manter a incrementalidade entre os backups. Sempre que um backup é feito, a Amazon FSx primeiro tira um instantâneo do seu volume. O snapshot do backup é armazenado em seu volume e consome espaço de armazenamento no volume. FSx Em seguida, a Amazon compara esse snapshot com o snapshot de backup anterior (se houver) e copia somente os dados alterados em seu backup.

Se não houver nenhum snapshot de backup anterior, todo o conteúdo do snapshot de backup mais recente será copiado ao backup. Depois que o último instantâneo de backup for obtido com sucesso, a Amazon FSx excluirá o instantâneo de backup anterior. O snapshot usado para o backup mais recente permanece no volume até que o próximo backup seja feito, quando o processo se repete. Para otimizar os custos com armazenamento de backup, o ONTAP preserva a economia de eficiência de armazenamento de um volume em seus backups.

Quando você exclui um backup, somente os dados exclusivos desse backup serão excluídos. Cada FSx backup da Amazon contém todas as informações necessárias para criar um novo volume a partir do backup, restaurando efetivamente um point-in-time instantâneo do volume.

Há limites para o número de backups que você pode armazenar por Conta da AWS volume. Para obter mais informações, consulte Cotas que podem ser aumentadas e Cotas de recursos para cada sistema de arquivos.

Requisitos de armazenamento

Seu volume e seu sistema de arquivos devem ter, cada um, capacidade de armazenamento SSD disponível suficiente para armazenar um snapshot de backup. Ao capturar o snapshot de backup, a capacidade adicional de armazenamento consumida pelo snapshot não poderá fazer com que o volume ultrapasse 98% de utilização do armazenamento SSD. Se isso acontecer, o backup falhará.

Você pode aumentar o armazenamento SSD de um volume ou o armazenamento SSD do sistema de arquivos a qualquer momento para garantir que seus backups não sejam interrompidos.

Backups automáticos diários

Quando você cria um sistema de arquivos, os backups diários automáticos são habilitados por padrão para os volumes do sistema de arquivos. É possível habilitar ou desabilitar a qualquer momento os backups diários automáticos para sistemas de arquivos existentes. Os backups diários automáticos de todos os volumes ocorrem durante a janela de backup diário do sistema de arquivos, que é definida automaticamente quando você cria um sistema de arquivos. É possível modificar a janela de backup diário a qualquer momento. Para um backup com desempenho ideal, recomendamos que você escolha uma janela de backup diário que esteja fora do horário normal de operação, quando clientes e aplicações estão acessando os dados em seus volumes.

Usando o console, você pode definir o período de retenção para backups diários automáticos com um valor de 1 a 90 dias ao criar um sistema de arquivos ou a qualquer momento. O período padrão de retenção para backups diários automáticos é de 30 dias. A Amazon FSx exclui um backup diário automático quando o período de retenção expira. Usando a API AWS CLI and, você pode definir o período de retenção em um valor de 0 a 90 dias; defini-lo como 0 desativa os backups diários automáticos.

Os backups diários automáticos, a janela de backup diário e o período de retenção de backup são configurações do sistema de arquivos e se aplicam a todos os volumes no sistema de arquivos. Você pode usar o FSx console da Amazon AWS CLI, o ou a API para alterar essas configurações. Para obter mais informações, consulte Atualizar sistemas de arquivos.

Você não pode criar um backup de volume (backups diários automáticos ou backups iniciados pelo usuário) se o volume estiver off-line. Para obter mais informações, consulte Como visualizar volumes off-line.

> **Note**
>
> Os backups diários automáticos têm um período máximo de retenção de 90 dias, mas os backups iniciados pelo usuário que você cria, que incluem backups criados usando, são retidos para sempre AWS Backup, a menos que você os exclua ou os AWS Backup exclua.

Você pode excluir manualmente um backup diário automático usando o FSx console, a CLI e a API da Amazon. Ao excluir um volume, você também exclui os backups diários automáticos desse

volume. A Amazon FSx oferece a opção de criar um backup final de um volume antes de você excluí-lo. O backup final é mantido para sempre, a menos que você o exclua.

Backups iniciados pelo usuário

Com a Amazon FSx, você pode fazer backups manualmente dos volumes do seu sistema de arquivos a qualquer momento usando a API AWS Management Console AWS CLI, e. Seus backups iniciados pelo usuário são incrementais em relação a outros backups que podem ter sido criados para um volume e são retidos para sempre, a menos que você os exclua. Os backups iniciados pelo usuário são retidos mesmo após excluir o volume ou o sistema de arquivos em que os backups foram criados. Você pode excluir backups iniciados pelo usuário somente usando o FSx console, a API ou a CLI da Amazon. Eles nunca são excluídos automaticamente pela Amazon FSx.

Para obter instruções sobre como criar um backup iniciado pelo usuário, consulte Como criar backups iniciados pelo usuário.

Copiar tags para backups

Ao criar ou atualizar um volume usando a CLI ou API, você pode habilitar `CopyTagsToBackups` para copiar automaticamente qualquer tag dos seus volumes para seus backups. No entanto, se você adicionar alguma tag ao criar um backup iniciado pelo usuário, incluindo nomear um backup ao usar o console, a Amazon FSx não copia as tags do volume, mesmo que `CopyTagsToBackups` esteja habilitado.

Usando AWS Backup com a Amazon FSx

AWS Backup é uma maneira simples e econômica de proteger seus dados fazendo backup de seus volumes Amazon FSx for NetApp ONTAP. AWS Backup é um serviço de backup unificado projetado para simplificar a criação, restauração e exclusão de backups, ao mesmo tempo em que fornece relatórios e auditoria aprimorados. O uso do AWS Backup facilita o desenvolvimento de uma estratégia centralizada de backup para fins de conformidade jurídica, regulamentar e profissional. Também simplifica a proteção AWS de seus volumes de armazenamento, bancos de dados e sistemas de arquivos, fornecendo um local central onde você pode fazer o seguinte:

- Configure e audite os AWS recursos dos quais você deseja fazer backup.
- Automatizar a programação de backups.
- Definir políticas de retenção.
- Monitore todas as atividades recentes de backup, cópia e restauração.

AWS Backup usa a funcionalidade de backup integrada da Amazon FSx. Os backups criados usando o AWS Backup console têm o mesmo nível de consistência e desempenho do sistema de arquivos, são incrementais em relação a qualquer outro backup do seu volume FSx iniciado pelo usuário da Amazon e oferecem as mesmas opções de restauração que os backups feitos usando o console da Amazon FSx . O uso AWS Backup para gerenciar esses backups fornece funcionalidade adicional, incluindo a capacidade de criar backups agendados com a mesma frequência a cada hora. Você pode adicionar uma camada extra de defesa para proteger os backups contra exclusões acidentais ou mal-intencionadas ao armazená-los em um cofre de backup.

Os backups criados por AWS Backup são considerados backups iniciados pelo usuário e contam para a cota de backup iniciada pelo usuário para a Amazon. FSx Para obter mais informações, consulte Cotas que podem ser aumentadas. Você pode visualizar e restaurar backups criados AWS Backup usando o FSx console, a CLI e a API da Amazon. No entanto, você não pode excluir backups criados AWS Backup no FSx console, na CLI ou na API da Amazon. Para obter mais informações, consulte Introdução AWS Backup no Guia do AWS Backup desenvolvedor.

AWS Backup não é possível fazer backup de volumes que estão off-line.

Você pode usar tags para selecionar quais dos seus FSx recursos do ONTAP estão protegidos em um plano de backup. Essas tags devem ser aplicadas no nível do volume e não no nível do sistema de arquivos como um todo. Para obter mais informações, consulte Atribuição de recursos a um plano de backup no Guia do AWS Backup desenvolvedor.

Restaurar backups em um novo volume

Você pode restaurar um backup de volume em um novo volume em um sistema de arquivos que esteja no mesmo Região da AWS em que o backup está armazenado. Você não pode restaurar um backup em um sistema de arquivos localizado em um local Região da AWS diferente do backup.

Ao restaurar um backup nos sistemas de arquivos FSx de segunda geração do ONTAP, os clientes podem montar e ler dados de um volume enquanto ele está sendo restaurado. Os clientes podem montar o volume que você está restaurando e ler os dados do arquivo depois que a Amazon FSx carrega todos os metadados no novo volume e o volume relata o status do ciclo de vida de. `CREATED` Você pode encontrar o estado do ciclo de vida de um volume na página de detalhes dos volumes no FSx console da Amazon e na resposta do comando describe-volumes da CLI.

Ao ler dados de um volume enquanto eles estão sendo restaurados de um backup, se os dados ainda não tiverem sido baixados para o volume, você terá latências de leitura de até dezenas de

milissegundos no primeiro acesso. Essas leituras são armazenadas em cache na camada SSD, e você pode esperar latências de leitura inferiores a um milissegundo para leituras subsequentes.

O tempo necessário para FSx a Amazon disponibilizar um volume para acesso somente leitura é proporcional à quantidade de metadados do arquivo armazenados no backup. Dependendo do tamanho médio do arquivo em seu conjunto de dados (conjuntos de dados de arquivos pequenos consomem mais metadados do que conjuntos de dados de arquivos grandes), os metadados de arquivo normalmente consomem de 1 a 7% dos dados gerais de backup.

Quando você restaura um backup de FlexGroup volume em um sistema de arquivos que tem um número diferente de pares de alta disponibilidade (HA) do sistema de arquivos original, a Amazon FSx adiciona volumes constituintes adicionais para garantir que os constituintes sejam distribuídos uniformemente.

> **Note**
>
> FSx A Amazon não oferece suporte ao acesso de leitura aos dados enquanto um volume está sendo restaurado a partir de um backup para SnapLock volumes ou para quaisquer volumes em sistemas de arquivos de primeira geração. Ao restaurar esses backups, o volume fica disponível para montar e acessar dados após a conclusão do processo de restauração, e todos os metadados e dados são carregados no novo volume.

Ao restaurar um backup, todos os dados são gravados inicialmente no nível de armazenamento SSD. Enquanto a restauração estiver em andamento, os dados serão hierarquizados no armazenamento do grupo de capacidade de acordo com a política de camadas do volume que estiver sendo restaurado. Como os dados são gravados primeiro no nível SSD, a Amazon FSx pausará o processo de restauração se o sistema de arquivos ficar sem espaço de armazenamento SSD. A restauração será retomada automaticamente assim que houver espaço suficiente no SSD disponível para continuar o processo. Se a política de camadas do volume restaurado for `All`, um processo periódico em segundo plano classificará os dados no grupo de capacidade. Se a política de camadas do volume restaurado for `Snapshot Only` ou `Auto`, os dados serão colocados em camadas no grupo de capacidade se a utilização do SSD no sistema de arquivos for maior que 50% e a taxa de resfriamento for determinada pelo período de resfriamento da política de camadas.

Se sua workload exigir latências de leitura consistentes de menos de um milissegundo ao restaurar um backup em um novo volume em sistemas de arquivos de segunda geração, recomendamos que você defina a política de hierarquização do volume como `None` ao iniciar a restauração e aguarde

até que todos os dados tenham sido totalmente baixados no volume antes de acessá-lo. Todos os dados serão carregados no armazenamento SSD antes de você tentar acessá-los, fornecendo acesso consistente de baixa latência aos seus dados.

Para step-by-step obter instruções sobre como restaurar um backup em um novo volume, consulteRestaurar um backup em um novo volume.

Em sistemas de arquivos de segunda geração, você também pode restaurar apenas um subconjunto de dados de um backup sem precisar esperar pela conclusão de toda a operação de restauração. A restauração de apenas um subconjunto dos dados de um backup permite que você retome as operações mais rapidamente no caso de exclusão, modificação ou corrupção acidental dos dados. Para obter mais informações, consulte Restaurar um subconjunto de dados.

Você pode monitorar o progresso ao restaurar um backup em um sistema de arquivos de segunda geração na AWS Management Console API AWS CLI, e. Para obter mais informações, consulte Monitorar o andamento ao restaurar um backup.

> **Note**
>
> - Você não pode criar um instantâneo de volume nem realizar operações baseadas em instantâneos, como clonagem, SnapMirror replicação e criação de backups de um volume enquanto ele está sendo restaurado a partir de um backup.
> - Um volume restaurado sempre tem o mesmo estilo de volume do volume original. Você não pode alterar o estilo do volume ao restaurar.

Desempenho de backup e restauração

Vários fatores podem influenciar o desempenho das operações de backup e restauração. As operações de backup e restauração são processos em segundo plano, o que significa que elas têm uma prioridade menor em relação às operações de E/S do cliente. As operações de E/S do cliente incluem leituras e gravações de dados e metadados NFS, CIFS e iSCSI. Todos os processos em segundo plano utilizam somente a parte não utilizada da capacidade de throughput do sistema de arquivos e podem levar de alguns minutos a algumas horas para terminar, dependendo do tamanho do backup e da quantidade de capacidade de throughput não utilizada do sistema de arquivos.

Outros fatores que afetam o desempenho do backup e da restauração incluem o nível de armazenamento no qual seus dados são armazenados e o perfil do conjunto de dados.

Recomendamos que você crie os primeiros backups de seus volumes quando a maioria dos dados estiver no armazenamento SSD. Os conjuntos de dados que contêm principalmente arquivos pequenos geralmente têm um desempenho inferior em comparação com conjuntos de dados de tamanho semelhante que contêm principalmente arquivos grandes. Isso ocorre porque o processamento de um grande número de arquivos pequenos consome mais ciclos de CPU e sobrecarga de rede do que processar menos arquivos grandes.

Geralmente, você pode esperar as seguintes taxas de backup ao fazer backup de dados armazenados no nível de armazenamento SSD:

- 750 MBps em vários backups simultâneos contendo principalmente arquivos grandes.
- 100 MBps em vários backups simultâneos contendo principalmente arquivos pequenos.

No geral, você pode esperar as seguintes taxas de restauração:

- 250 MBps em várias restaurações simultâneas contendo principalmente arquivos grandes.
- 100 MBps em várias restaurações simultâneas contendo principalmente arquivos pequenos.

Fazer o backup de volumes do SnapLock

Você pode fazer o backup de volumes do SnapLock para obter proteção adicional de dados. Ao restaurar um volume do SnapLock, as configurações originais do volume, como a retenção padrão, a retenção mínima e a retenção máxima, são preservadas. As configurações de gravação única e várias leituras (WORM) e de retenção jurídica também são preservadas.

> **Note**
>
> Você não pode fazer backup de um volume SnapLock FlexGroup.

Você pode restaurar o backup de um volume do SnapLock como um volume do SnapLock ou que não seja do SnapLock. No entanto, você não pode restaurar o backup de um volume que não seja do SnapLock como um volume do SnapLock.

Para obter mais informações, consulte Como SnapLock funciona.

Como criar backups iniciados pelo usuário

O procedimento a seguir descreve como criar um backup de um volume iniciado pelo usuário.

Você não pode criar um backup de volume se o volume estiver off-line. Para obter mais informações, consulte Como visualizar volumes off-line.

Para criar um backup iniciado pelo usuário (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Acesse Sistemas de arquivos e escolha o sistema de arquivos do ONTAP para o qual você deseja fazer backup de um volume.
3. Escolha a guia Volumes.
4. Escolha o volume do qual deseja fazer o backup.
5. Em Ações, escolha Criar backup.
6. Na caixa de diálogo Criar backup que é aberta, forneça um nome para o backup. Os nomes de backup podem ter no máximo 256 caracteres Unicode, incluindo letras, espaço em branco, números e os caracteres especiais . + - = _ : /
7. Escolha Create backup.

Você acaba de criar um backup de um dos volumes do sistema de arquivos. Você pode ver todos os seus backups no FSx console da Amazon escolhendo Backups na navegação do lado esquerdo. Você pode pesquisar pelo nome que deu ao backup e pelos filtros da tabela para mostrar apenas os resultados correspondentes.

Ao criar um backup iniciado pelo usuário conforme descrito neste procedimento, ele terá o tipo `USER_INITIATED` e o status `CREATING` até que esteja totalmente disponível.

Restaurar um backup em um novo volume

Os procedimentos a seguir descrevem como restaurar um FSx backup do ONTAP em um novo volume usando o AWS Management Console e. AWS CLI Ao restaurar um volume em um sistema de arquivos de segunda geração, você pode monitorar o progresso usando a AWS Management Console API AWS CLI, e.

Para restaurar um backup de volume em um novo volume (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.

2. No painel de navegação, escolha Backups e, em seguida, escolha o backup FSx de volume do ONTAP que você deseja restaurar.
3. No menu Ações no canto superior direito, escolha Restaurar backup. A página Criar volume a partir do backup é exibida.
4. Escolha a FSx máquina virtual do sistema de arquivos e armazenamento ONTAP para a qual você deseja restaurar o backup nos menus suspensos.
5. No menu Ações no canto superior direito, escolha Restaurar backup. A página Criar volume a partir do backup é exibida.
6. Escolha a FSx máquina virtual do sistema de arquivos e armazenamento ONTAP para a qual você deseja restaurar o backup nos menus suspensos.
7. Em Detalhes do volume, há várias seleções. Primeiro, insira o Nome do volume. Você pode usar até 203 caracteres alfanuméricos ou sublinhado (_).
8. Em Tamanho do volume, insira qualquer número inteiro no intervalo de 20 a 314572800 para especificar o tamanho em mebibytes (MiB).
9. Em Tipo de volume, escolha Leitura/gravação (RW) para criar um volume passível de leitura e gravação, ou Proteção de dados (DP) para criar um volume somente leitura e que possa ser usado como o destino de um relacionamento SnapMirror ou SnapVault do NetApp. Para obter mais informações, consulte Tipos de volume.
10. Em Caminho da junção, insira um local no sistema de arquivos para montar o volume. O nome deve ter uma barra inicial, por exemplo `/vol3`.
11. Em Eficiência de armazenamento, escolha Habilitado para habilitar os recursos de eficiência de armazenamento do ONTAP (desduplicação, compressão e compactação). Para obter mais informações, consulte Eficiência de armazenamento.
12. Em Estilo de segurança do volume, escolha Unix (Linux), NTFS ou Misto. O estilo de segurança de um volume determina se é dada preferência ao NTFS ou ao UNIX ACLs para acesso multiprotocolo. O modo MISTO não é necessário para acesso multiprotocolo e só é recomendado para usuários avançados.
13. Em Política de snapshots, escolha uma política de snapshots para o volume. Para obter mais informações sobre políticas de snapshots, consulte Políticas de snapshots.

    Se você escolher Política personalizada, especifique o nome da política no campo política personalizada. A política personalizada já deve existir na SVM ou no sistema de arquivos. Você pode criar uma política de snapshots personalizada com a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política Snapshot na documentação do produto do NetApp ONTAP.

14. Em Período de resfriamento da política de divisão em níveis, os valores válidos são de 2 a 183 dias. O período de resfriamento da política de camadas de um volume define o número de dias antes que os dados que não foram acessados sejam marcados como frios e movidos para o armazenamento do grupo de capacidade. Essa configuração afeta somente as políticas `Auto` e `Snapshot-only`.
15. Na seção Avançado, em Configuração do SnapLock, você pode deixar a configuração padrão Desabilitado ou escolher Habilitado para configurar um volume SnapLock. Para obter mais informações sobre como configurar um volume do SnapLock Compliance ou do SnapLock Enterprise, consulte Noções básicas SnapLock Compliance e Noções básicas SnapLock Enterprise. Para obter mais informações sobre o SnapLock, consulte Protegendo seus dados com SnapLock.
16. Escolha Confirmar para criar o volume.
17. Se você estiver restaurando o backup em um sistema de arquivos de segunda geração, poderá monitorar o andamento da restauração do backup na guia Atualizações na página Volume. Para obter mais informações, consulte Monitorar o andamento ao restaurar um backup.

Para restaurar um backup em um novo volume (CLI)

Use o comando create-volume-from-backupCLI ou o comando de CreateVolumeFromBackupAPI equivalente para restaurar um backup de volume em um novo volume.

- ```
  $ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
        --name demo --ontap-configuration JunctionPath=/demo,SizeInMegabytes=100000,\
        StorageVirtualMachineId=svm-0f04a9c7c27e1908b,TieringPolicy={Name=ALL}
  ```

  A resposta do sistema para uma solicitação de restauração bem-sucedida para restaurar um backup em um sistema de arquivos de segunda geração é a seguinte. A resposta inclui o objeto `"AdministrativeActions"` que fornece informações de status e andamento sobre a solicitação.

  ```
  {
        "Volume": {
            "CreationTime": 1692721488.428,
            "FileSystemId": "fs-07ab735385276ed60",
            "Lifecycle": "CREATING",
            "Name": "demo",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
  ```
  ```

```
            "JunctionPath": "/demo",
            "SizeInMegabytes": 100000,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "ALL"
            },
            "OntapVolumeType": "DP",
            "SnapshotPolicy": "default",
            "CopyTagsToBackups": false,
        },
        "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
        "VolumeId": "fsvol-0b6ec764c9c5f654a",
        "VolumeType": "ONTAP",
  --->  "AdministrativeActions": [
            {
                "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
                "RequestTime": 1685729972.069,
                "Status": "PENDING"
            }
        ]               <----
    }
}
```

A resposta do sistema para uma solicitação bem-sucedida de restauração de um backup em um sistema de arquivos de primeira geração é a seguinte.

```
{
    "Volume": {
        "CreationTime": 1692721488.428,
        "FileSystemId": "fs-07ab735385276ed60",
        "Lifecycle": "CREATING",
        "Name": "demo",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/demo",
            "SizeInMegabytes": 100000,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
```

```
                    "Name": "ALL"
                },
                "OntapVolumeType": "DP",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
            },
            "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
            "VolumeId": "fsvol-0b6ec764c9c5f654a",
            "VolumeType": "ONTAP",
        }
    }
```

Ao restaurar um volume em um sistema de arquivos de segunda geração, você pode monitorar o progresso usando a AWS Management Console API AWS CLI, e.

Restaurar um subconjunto de dados

Você pode restaurar um subconjunto de dados de um backup enquanto ele está sendo restaurado em um novo volume em sistemas de arquivos de segunda geração sem precisar esperar até que todo o conjunto de dados de backup tenha sido totalmente restaurado.

O procedimento a seguir lista as etapas a serem seguidas quando você precisar recuperar um subconjunto de dados ao restaurar um backup e não puder aguardar a conclusão de toda a restauração:

Para restaurar um subconjunto de dados ao restaurar um backup

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Na página Backups, localize o backup que contém a versão dos dados que deseja restaurar.
3. No menu Ações no canto superior direito, escolha Restaurar backup. A página Criar volume a partir do backup é exibida.
4. Escolha a FSx máquina virtual do sistema de arquivos e armazenamento ONTAP para a qual você deseja restaurar o backup nos menus suspensos.
5. Em Detalhes do volume, configure o volume para atender às suas necessidades.
6. Escolha Confirmar para criar o volume.
7. Monitore o andamento da restauração do backup.
8. Monte o volume que está sendo restaurado quando ele exibir o status do ciclo de vida `CREATED`.

9. Localize o subconjunto de dados no volume que você precisa copiar.
10. Copie os dados para o volume existente que sua aplicação usa.
11. Depois que os dados necessários do backup forem copiados para o local de destino, você poderá excluir o volume que está sendo restaurado antes da conclusão a fim de otimizar a utilização dos recursos do sistema de arquivos.

Monitorar o andamento ao restaurar um backup

Você pode monitorar o progresso ao restaurar um backup de volume no sistema de arquivos de segunda geração na API AWS Management Console, AWS CLI, e. Como em todas as ações FSx administrativas da Amazon, um status de restauração de backup está disponível no console, na CLI e na API por 30 dias após a conclusão da operação.

Para monitorar o andamento ao restaurar um backup (console)

Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.

1. No menu de navegação à esquerda, escolha Volumes.
2. Escolha o volume para o qual o backup está sendo restaurado.
3. Escolha a guia Atualizações.
4. O Tipo de atualização Backup e restauração fornece as seguintes informações:

    - PENDING indica que os metadados do arquivo estão sendo baixados no volume. O Estado do ciclo de vida do volume é CREATING.
    - IN_PROGRESS indica que o volume está disponível e que os clientes podem montar o volume com acesso somente leitura aos dados. A % de andamento mostra a porcentagem de dados que foram baixados para o volume.
    - COMPLETED indica que todos os dados foram baixados para o volume e que a restauração do backup foi concluída. Agora, os clientes têm acesso de leitura e gravação. Para volumes `RW`, o tipo do volume muda de `DP` para `RW` nesse momento.

Para monitorar o andamento ao restaurar um backup (CLI)

- Ao restaurar um backup em um novo volume em um sistema de arquivos ONTAP FSx de segunda geração, você pode monitorar o progresso da restauração usando o comando CLI `describe-volumes`.

Ao restaurar um backup em um sistema de arquivos de segunda geração, a resposta inclui o objeto `AdministrativeActions`, que fornece informações de status sobre o processo de download de dados. A ferramenta

```
$ aws fsx describe-volumes
{
    “Volumes”: [
        {
            “CreationTime”: 1691686114.674,
            “FileSystemId”: fs-029ff92192bd4d375,
            “LifeCycle”: “CREATING”,
            “Name”: vol1,
            “OntapConfiguration”: {
                   “FlexCacheEndpointType”: “NONE”,
                   “JunctionPath”: “/vol1”,
                   “SizeInMegabytes”: 100000,
                   “StorageEfficiencyEnabled”: true,
                   “StorageVirtualMachineId”: “svm-0ed1d714019426ca9”,
                   “StorageVirtualMachineRoot”: false,
                   “TieringPolicy”: {
                    “Name”: “ALL”
                   },
                   “OntapVolumeType”: “DP”,
                   “SnapshotPolicy”: “default”,
                   “CopyTagsToBackups”: false,
                  },
                  “ResourceARN”: “arn:aws:fsx:us-east-1:630831496844:volume/
fs-08ac75f715c6aec76/fsvol-094c015af930790fa”,
                  “VolumeId”: “fsvol-094c015af930790fa”,
                  “VolumeType”: “ONTAP”,
                  “AdministrativeActions”: [
                         {
                          “AdministrativeActionType”: “DOWNLOAD_DATA_FROM_BACKUP”,
                          “RequestTime”: 1685729972.069,
                          “Status”: “PENDING”
                         }
                  ]
    }
```

Depois que a Amazon FSx carrega todos os metadados do arquivo no volume restaurado, esses campos têm os seguintes valores:

- `"LifeCycle": "CREATED"`: indica que o volume está pronto para ser montado.
- `"OntapVolumeType": "DP"`: indica que o volume é somente leitura durante o download dos dados do arquivo.
- `"ProgressPercent`: mostra a porcentagem de dados do arquivo que são carregados no volume.
- `"Status": "IN_PROGRESS"`: o download dos dados do arquivo para o volume está em andamento.

Nesse estágio do processo de restauração, você pode montar o volume com acesso somente leitura a todos os dados do backup que você está restaurando.

Quando a Amazon concluir FSx o download de todos os dados do arquivo no novo volume, os clientes terão acesso total de leitura e gravação, se esse for `RW` o volume. Os indicadores têm os seguintes valores:

- `"LifeCycle": "CREATED"`: inalterado
- `"OntapVolumeType": "RW"`: indica que os clientes têm acesso total de leitura e gravação.
- `"Status": "COMPLETED"`: indica que a restauração foi concluída.

Se o processo de restauração falhar, o `AdminstrativeAction > Status` terá um valor de `FAILED`. Uma mensagem de erro é fornecida no objeto `FailureDetails`. Para obter mais informações, consulte AdministrativeActionFailureDetailsna Amazon FSx API Reference

Excluir backups

Você pode excluir backups diários automáticos e backups iniciados pelo usuário de seus volumes usando o FSx console da Amazon, a FSx API da Amazon ou AWS Command Line Interface (AWS CLI). A exclusão de um backup é uma ação permanente e irrecuperável. Todos os dados em um backup excluído também são excluídos. Não exclua um backup, a menos que tenha certeza de que não precisará dele novamente no futuro. Você não pode excluir um backup se o volume de origem estiver off-line.

Você pode excluir um volume enquanto ele está sendo restaurado a partir de um backup em todos os sistemas FSx de arquivos ONTAP. A exclusão de um volume durante a restauração cancela efetivamente a operação de restauração em andamento.

> **Note**
>
> A Amazon FSx não oferece suporte à exclusão do `AVAILABLE` backup mais recente de um ONTAP volume, a menos que todos os outros backups do volume tenham sido excluídos.

Para excluir backups criados usando AWS Backup, consulte Excluindo backups no Guia do AWS Backup desenvolvedor.

Para excluir um backup (console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel do console, escolha Backups na navegação do lado esquerdo.
3. Escolha o backup que você deseja excluir da tabela Backups e, em seguida, escolha Excluir backup.
4. Na caixa de diálogo Excluir backups que é exibida, confirme se o ID do backup exibido é do backup que você deseja excluir.
5. Confirme se a caixa de seleção do backup que deseja excluir está marcada.
6. Escolha Excluir backups.

Seu backup e todos os dados incluídos agora foram excluídos de forma permanente e irrecuperável.

Para excluir um backup (CLI)

- Use o comando da CLI delete-backup ou a ação de API DeleteBackup equivalente para excluir FSx um backup de volume for ONTAP, conforme mostrado no exemplo a seguir.

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

A resposta do sistema inclui o ID do backup que está sendo excluído e seu status do ciclo de vida com um valor de `DELETED`, indicando que a solicitação foi bem-sucedida.

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

Como proteger seus dados com snapshots

Um snapshot é uma imagem somente para leitura de um volume Amazon FSx for NetApp ONTAP em um determinado momento. Os snapshots oferecem proteção contra exclusão ou modificação acidental de arquivos nos volumes. Com os snapshots, seus usuários podem visualizar e restaurar facilmente arquivos individuais ou pastas de um snapshot anterior para desfazer alterações, recuperar conteúdo excluído e comparar versões de arquivo.

Um snapshot contém os dados que foram alterados desde o último snapshot, o que consome a capacidade de armazenamento SSD do sistema de arquivos. Os snapshots não estão incluídos em nenhum backup de volume. Os snapshots são habilitados por padrão nos volumes usando a política de snapshots `default`. Os snapshots são armazenados no diretório `.snapshot` na raiz de um volume. Você pode armazenar até 1.023 snapshots por volume em qualquer ponto no tempo. Após atingir esse limite, você deverá excluir um snapshot existente antes que um novo snapshot do volume possa ser criado.

Tópicos

- Políticas de snapshots
- Restauração de arquivos com base em snapshots
- Visualizar o snapshot comum
- Atualizar a reserva de snapshots do seu volume
- Desabilitar snapshots automáticos
- Exclusão de snapshots
- Exclusão de snapshots
- Reserva de snapshot

Políticas de snapshots

A política de snapshots define como o sistema cria snapshots para um volume. A política especifica quando criar snapshots, quantas cópias devem ser retidas e como dar nomes a elas. Há três políticas de snapshot integradas FSx para o ONTAP:

- `default`
- `default-1weekly`
- `none`

Por padrão, cada volume está associado à política de snapshots `default` do sistema de arquivos. Recomendamos usar essa política para a maioria das workloads.

A política `default` cria snapshots automaticamente de acordo com a programação a seguir, com as cópias mais antigas de snapshots excluídas para liberar espaço para cópias mais recentes.

- No máximo seis snapshots por hora, feitos cinco minutos depois da hora.
- No máximo dois snapshots por dia, feitos de segunda a sábado, 10 minutos depois da meia-noite.
- No máximo dois snapshots por semana, feitos todos os domingos, 15 minutos depois da meia-noite.

> **Note**
>
> Os horários dos snapshots são baseados no fuso horário do sistema de arquivos, cujo padrão é o Tempo Universal Coordenado (UTC). Você pode definir um fuso horário FSx para o sistema de arquivos ONTAP usando o comando `timezone -timezone` *`time_zone`* ONTAP CLI. Para obter mais informações sobre como acessar a ONTAP CLI, consulte. Usar o NetApp ONTAP CLI

A política `default-1weekly` funciona da mesma maneira que a política `default`, exceto por reter apenas um snapshot da agenda semanal.

A política none não cria nenhum snapshot. Essa política pode ser atribuída a volumes para evitar que snapshots automáticos sejam criados.

Você também pode criar uma política de snapshots personalizada usando a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política de snapshot na documentação do produto NetApp ONTAP. Você pode escolher uma política de snapshot ao criar ou atualizar um volume no FSx console da Amazon AWS CLI, no ou na FSx API da Amazon. Para obter mais informações, consulte Como criar volumes e Atualizar volumes.

Restauração de arquivos com base em snapshots

Usando os snapshots em seu sistema de FSx arquivos da Amazon, você pode restaurar rapidamente versões anteriores de arquivos ou pastas individuais.

Se usar clientes Linux e macOS, você poderá visualizar snapshots no diretório `.snapshot` na raiz de um volume. Se usar clientes Windows, você poderá visualizar snapshots na guia `Previous Versions` do Windows Explorer (ao clicar com o botão direito do mouse em um arquivo ou pasta).

Restaurar um arquivo usando um snapshot (clientes Linux e macOS)

1. Se o arquivo original ainda existir e você não quiser substituí-lo pelo arquivo em um snapshot, use o cliente Linux ou macOS para renomear o arquivo original ou movê-lo para outro diretório.
2. No diretório `.snapshot`, localize o snapshot que contém a versão do arquivo que deseja restaurar.
3. Copie o arquivo do diretório `.snapshot` para o diretório no qual o arquivo existia originalmente.

Restaurar um arquivo usando um snapshot (clientes Windows)

Os usuários de clientes Windows podem restaurar arquivos para versões anteriores usando a interface familiar do Explorador de Arquivos do Windows.

1. Para restaurar um arquivo, os usuários escolhem o arquivo a ser restaurado e selecionam Restaurar versões anteriores no menu de contexto (clique com o botão direito do mouse).
2. Os usuários podem então visualizar e restaurar uma versão anterior na lista Versões anteriores.

Os dados em snapshots são somente leitura. Se quiser fazer modificações nos arquivos e pastas listados na guia Versões anteriores, é necessário salvar uma cópia dos arquivos e pastas que deseja modificar em um local gravável e fazer modificações nas cópias.

Visualizar o snapshot comum

O snapshot comum é usado para manter a incrementalidade entre os seus backups. Este procedimento explica como identificar o snapshot comum no volume.

Para visualizar o snapshot comum de um volume

- Para determinar qual snapshot é o snapshot comum de um volume, use o comando volume snapshot showda CLI do ONTAP.

```
volume snapshot show -volume volume-name
```

Na saída, o nome do instantâneo comum tem o formato de`backup-id`, onde *`id`* é uma sequência alfanumérica de 17 dígitos, conforme mostrado no exemplo a seguir:

```
FsxIdabc12345::> volume snapshot show -volume test_vol
                                  ---Blocks---
Vserver Volume    Snapshot                    Size     Total% Used%
-------- -------- -------------------------- -------- ------ -----
dest-svm test_vol
                  snap1                       144KB    0%     3%
                  snap2                       832KB    0%    16%
         --->     backup-abcdef0123456789a   4.87MB    0%    53% <---
                  weekly.2024-05-26_0015     5.02MB    0%    54%
                  weekly.2024-06-02_0015     2.22MB    0%    34%
                  daily.2024-06-04_0010       284KB    0%     6%
                  daily.2024-06-05_0010      4.29MB    0%    50%
                  hourly.2024-06-05_0705      168KB    0%     4%
8 entries were displayed.
```

Important

Não exclua o snapshot comum no volume, pois ele é usado para manter a incrementalidade entre os seus backups. A exclusão do snapshot comum de um volume fará com que o próximo backup seja um backup completo do volume em vez de um backup incremental.

Atualizar a reserva de snapshots do seu volume

Você pode alterar a quantidade de reserva de snapshot em um volume usando a CLI ou a API do NetApp ONTAP, descrita no procedimento a seguir.

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Use o comando `volume modify` da CLI do ONTAP para alterar a porcentagem de espaço em disco usada para a reserva de cópias do snapshot. Substitua os seguintes valores de espaço reservado por seus dados:

   - *svm_name*: use o nome da sua SVM.
   - *vol_name*: use o nome do seu volume.
   - *percent*: a porcentagem de espaço em disco que você deseja reservar para cópias do snapshot.

   ```
   ::> volume modify -vserver svm_name -volume vol_name -percent-snapshot-
   space percent
   ```

   O exemplo a seguir altera a reserva de snapshot de vol1 para 25% da capacidade de armazenamento do volume.

   ```
   ::> volume modify -vserver vs0 -volume vol1 -percent-snapshot-space 25
   ```

Desabilitar snapshots automáticos

Os instantâneos automáticos são habilitados pela política de instantâneos padrão para volumes em seu FSx sistema de arquivos do ONTAP. Se você não precisar de instantâneos dos seus dados (por exemplo, se estiver usando dados de teste), poderá desabilitar os instantâneos definindo a política de instantâneos do volume para none usar a API AWS Management Console, a API AWS CLI e a ONTAP CLI, conforme descrito nos procedimentos a seguir.

Para desativar os instantâneos automáticos (AWS console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do ONTAP para o qual deseja atualizar um volume.
3. Escolha a guia Volumes.
4. Escolha o volume que deseja atualizar.
5. Em Ações, escolha Atualizar volume.

   A caixa de diálogo Atualizar volume é exibida com as configurações atuais do volume.

6. Em Política de snapshot, selecione Nenhuma.
7. Selecione Atualizar para atualizar o volume.

Para desativar os instantâneos automáticos (AWS CLI)

- Use o comando da AWS CLI update-volume (ou o comando equivalente da UpdateVolumeAPI) para definir o comonone, conforme mostrado no exemplo `SnapshotPolicy` a seguir.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=none, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Para desabilitar os snapshots automáticos (CLI do ONTAP)

Defina a política de snapshots do volume para usar a política padrão none para desabilitar os snapshots automáticos.

1. Use o comando `volume snapshot policy show` da CLI do ONTAP para mostrar a política none.

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                         Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ----------------------------------
none                               0 false   Policy for no automatic snapshots.
    Schedule               Count     Prefix                SnapMirror Label
    ---------------------- -----     --------------------- -------------------
    -                          -     -                     -
```

2. Use o comando `volume modify` da CLI do ONTAP para definir a política de snapshots do volume como none para desativar os snapshots automáticos. Substitua os seguintes valores de espaço reservado por seus dados:

   - *svm_name*: use o nome da sua SVM.

- *vol_name*: use o nome do seu volume.

Quando for solicitado que continue, insira **y**.

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none

Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
 Snapshot copies on this volume
        that do not match any of the prefixes of the new Snapshot policy will not
 be deleted. However, when
        the new Snapshot policy takes effect, depending on the new retention
 count, any existing Snapshot copies
        that continue to use the same prefixes might be deleted. See the 'volume
 modify' man page for more information.
Do you want to continue? {y|n}: y
Volume modify successful on volume vol_name of Vserver svm_name.
```

Exclusão de snapshots

Os snapshots consomem capacidade de armazenamento somente para os dados em um volume que tenham mudado desde o último snapshot. Por esse motivo, se sua workload gravar dados rapidamente, os snapshots de dados antigos podem ocupar uma quantidade significativa da capacidade de armazenamento de um volume.

Por exemplo, a saída do comando `volume show-space` da CLI do ONTAP mostra 140 KB de `User Data`. No entanto, o volume tinha 9,8 GB de `User Data` antes de os dados do usuário serem excluídos. Mesmo que você tenha excluído os arquivos do volume, um snapshot ainda pode fazer referência a dados antigos do usuário. Por esse motivo, `Snapshot Reserve` e `Snapshot Spill` no exemplo anterior, ocupam um total de 9,8 GB de espaço, embora praticamente não haja dados do usuário no volume.

Para liberar espaço nos volumes, você pode excluir snapshots mais antigos que não são mais necessários. Como os snapshots são incrementais, você não recupera a quantidade de armazenamento igual ao tamanho do snapshot ao excluí-lo. Você pode ver a quantidade de armazenamento que você pode recuperar ao excluir um snapshot usando o comando CLi do volume snapshot compute-reclaimable -vserverONTAP, usando seus dados para substituir, e. *svm_name vol_name snapshot_name*

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

É possível excluir snapshots criando uma política de exclusão automática de snapshots ou excluindo snapshots manualmente. A exclusão de um snapshot exclui os dados alterados armazenados no snapshot.

Exclusão de snapshots

Use o comando volume snapshot delete da CLI do ONTAP para excluir manualmente os snapshots, substituindo os seguintes valores de espaço reservado pelos seus dados:

- Substitua *svm_name* pelo nome da SVM na qual o volume foi criado.
- Substitua *vol_name* pelo nome do volume.
- Substitua *snapshot_name* pelo nome do snapshot. Esse comando é compatível com caracteres curinga (*) para *snapshot_name*. Portanto, você pode excluir todos os snapshots de hora em hora, por exemplo, usando `hourly*`.

> **Important**
>
> Se você tiver os FSx backups da Amazon habilitados, a Amazon FSx retém um snapshot do FSx backup mais recente da Amazon de cada volume. Esses snapshots são usados para manter a incrementalidade entre os backups e não devem ser excluídos usando esse método. Para obter mais informações, consulte Visualizar o snapshot comum.

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

Como criar uma política de exclusão automática de snapshots

Você pode criar uma política para excluir automaticamente os snapshots quando a quantidade de espaço disponível no volume estiver acabando. Use o comando volume snapshot autodelete modify da CLI do ONTAP para estabelecer uma política de exclusão automática para um volume.

Ao usar esse comando, use seus dados para substituir os seguintes valores de espaço reservado:

- Substitua *svm_name* pelo nome da SVM na qual o volume foi criado.
- Substitua *vol_name* pelo nome do volume.

Para `-trigger`, atribua um dos valores a seguir.

- `volume`: use `volume` se quiser que o limite no qual os snapshots são excluídos corresponda a um limite de capacidade total do volume usado. Os limites de capacidade do volume usado que acionam a exclusão do snapshot são determinados pelo tamanho do volume, com o limite sendo escalonado de 85 a 98% da capacidade usada. Volumes menores têm um limite menor e volumes maiores têm um limite maior.
- `snap_reserve`: use `snap_reserve` se quiser que os snapshots sejam excluídos com base no que pode ser mantido na sua reserva de snapshots.

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true
 -trigger [volume|snap_reserve]
```

Para obter mais informações, consulte o comando volume snapshot autodelete modify no Centro de Documentação do NetApp ONTAP.

Reserva de snapshot

A reserva de cópias de snapshot define uma porcentagem específica da capacidade de armazenamento de um volume para armazenar cópias instantâneas, com um valor padrão de 5%. A reserva de cópias de snapshot deve ter espaço suficiente alocado para as cópias de snapshot, incluindo backups de volume. Se as cópias de snapshot excederem o espaço de reserva de snapshot, você deverá excluir as cópias existentes do sistema de arquivos ativo para recuperar a capacidade de armazenamento para uso do sistema de arquivos. Você também pode modificar a porcentagem de espaço em disco alocada às cópias de snapshot.

Sempre que os snapshots consumirem mais de 100% da reserva de snapshots, eles começarão a ocupar espaço de armazenamento no SSD principal. Esse processo é chamado de vazamento de snapshot. Quando os snapshots continuarem ocupando o espaço ativo do sistema de arquivos, o sistema de arquivos correrão o risco de ficar cheio. Se o sistema de arquivos ficar cheio devido ao vazamento de snapshots, você só poderá criar arquivos depois de excluir snapshots suficientes.

Quando houver espaço em disco suficiente para snapshots na reserva de snapshots, a exclusão de arquivos do nível do SSD principal liberará espaço em disco para novos arquivos, enquanto

as cópias de snapshots que fazem referência a esses arquivos consomem somente o espaço na reserva de cópias de snapshots.

Como não é possível evitar que os snapshots consumam espaço em disco maior do que a quantidade reservada para eles (a reserva de snapshots), é importante reservar espaço em disco suficiente para os snapshots, de modo que a camada SSD principal sempre tenha espaço disponível para criar novos arquivos ou modificar os existentes.

Se um snapshot for criado quando os discos estiverem cheios, a exclusão de arquivos da camada SSD principal não criará nenhum espaço livre, pois todos esses dados também serão referenciados pelo snapshot recém-criado. Você deve excluir o snapshot para liberar espaço de armazenamento a fim de criar ou atualizar qualquer arquivo.

Você pode modificar a quantidade de reserva de snapshot em um volume usando a CLI do NetApp ONTAP. Para obter mais informações, consulte Atualizar a reserva de snapshots do seu volume.

Protegendo seus dados com a Proteção Autônoma contra Ransomware

A Proteção Autônoma contra Ransomware (ARP) é uma NetApp ONTAP Recurso orientado por IA que monitora e protege seus dados contra ataques de ransomware e malware se seus clientes Windows ou Linux ficarem comprometidos. Usando o aprendizado de máquina, o ARP se familiariza com seus FSx sistemas de arquivos ONTAP para detectar proativamente atividades anormais. O ARP está disponível para todos os sistemas de arquivos novos e existentes FSx do ONTAP em todos os lugares onde o Regiões da AWS Amazon FSx for NetApp ONTAP está disponível.

Como funciona o ARP

Você pode habilitar o ARP por volume ou, por padrão, em todos os novos volumes em uma SVM usando o ONTAP CLI ou API REST. Para obter mais informações sobre como habilitar o ARP, consulteHabilitando a proteção autônoma contra ransomware.

O ARP opera em dois modos: aprendizado e ativo. Quando você ativa o ARP pela primeira vez para seu volume FSx para ONTAP, ele é executado no modo de aprendizado. No modo de aprendizado, o ARP analisa seus padrões de acesso à carga de trabalho. ONTAP determina automaticamente o período de aprendizado ideal com base na carga de trabalho do seu volume, que pode levar até 30 dias. Quando isso é feito, o ARP passa para o modo ativo. No modo ativo, o ARP monitora

os dados recebidos e a atividade no volume para identificar possíveis ataques de ransomware e malware. Para obter mais informações, consulte O que o ARP procura. Se o ARP detectar alguma atividade anormal, um ONTAP Um snapshot é criado automaticamente para ajudá-lo a recuperar seus dados o mais próximo possível do momento do possível ataque. O instantâneo terá um prefixo de`Anti_ransomware_backup`, por isso é fácil de identificar. Se for determinado que a probabilidade de ataque é moderada, ONTAP gerará uma mensagem do Sistema de Gerenciamento de Eventos (EMS) para você revisar. Para obter mais informações, consulte Como responder a um ataque suspeito com o ARP e Entendendo os alertas do EMS para proteção autônoma contra ransomware.

A sobrecarga de desempenho do ARP é mínima para a maioria das cargas de trabalho. Se seus volumes tiverem cargas de trabalho de leitura intensiva, NetApp recomenda proteger no máximo 150 desses volumes por sistema de arquivos. Se você exceder esse número, o IOPS dessa carga de trabalho poderá cair em até 4%. Se seus volumes tiverem cargas de trabalho intensivas em gravação, NetApp recomenda proteger no máximo 60 desses volumes por sistema de arquivos. Caso contrário, o IOPS dessa carga de trabalho poderá cair em até 10%. Para obter mais informações sobre desempenho, consulte Amazon FSx para desempenho do NetApp ONTAP.

Não há custo adicional para habilitar o ARP em seu sistema de arquivos FSx for ONTAP.

O que o ARP procura

O ARP procura sinais de que seus clientes Windows ou Linux estão comprometidos. Depois que o ARP conhece seu volume FSx para ONTAP e muda para o modo ativo, ele procura os seguintes tipos de atividade no volume:

- Mudanças na entropia, o que significa diferenças na aleatoriedade dos dados em um arquivo.
- Alterações nos tipos de extensão de arquivo, o que significa que a nova extensão não é consistente com o tipo de extensão normalmente usado. O padrão é 20 arquivos com extensões de arquivo não observadas anteriormente no volume.
- Alterações no IOPS do arquivo, o que significa um aumento na atividade anormal do volume com dados criptografados.

Você pode modificar os parâmetros de detecção de ransomware do seu volume, se necessário. Por exemplo, se seu volume hospeda vários tipos de extensões de arquivo. Para obter mais informações, consulte Gerenciar os parâmetros de detecção de ataques do ONTAP Autonomous Ransomware Protection no Centro de NetApp Documentação.

> **Note**
>
> O ARP não impede que administradores desonestos com credenciais acessem seu FSx sistema de arquivos do ONTAP. AWS recomenda uma abordagem de segurança em camadas, incluindo, AWS BackupONTAP instantâneos e SnapLock.

Como responder a um ataque suspeito com o ARP

Se o ARP detectar um ataque, ele gerará um instantâneo que pode ser usado como ponto de recuperação. O instantâneo está bloqueado e não pode ser excluído normalmente. Dependendo da gravidade do ataque, ele também gerará um alerta EMS que mostra o volume afetado, a probabilidade do ataque e o cronograma do ataque. Se quiser receber alertas para a criação de um novo instantâneo ou a observação de uma nova extensão de arquivo em seu volume, você pode configurar o ARP para enviar esses alertas. Para obter mais informações, consulte Configurar alertas ARP no Centro de NetApp Documentação.

Você pode gerar um relatório para ver informações detalhadas sobre um ataque suspeito. Depois de revisar o relatório, você pode dizer ONTAP se o alerta foi gerado por um falso positivo ou por um ataque suspeito. Se você rotular o alerta como um ataque suspeito, deverá determinar o escopo do ataque e, em seguida, recuperar os dados do instantâneo criado pelo ARP. Se você rotular o ataque como falso positivo, o instantâneo criado pelo ARP será automaticamente excluído. Para obter mais informações, consulte Respondendo aos alertas da Autonomous Ransomware Protection.

Recomendamos monitorar as mensagens EMS do seu sistema de arquivos e o status dos seus volumes no ONTAP CLI e API REST. Para obter mais informações sobre mensagens EMS para ARP, consulteEntendendo os alertas do EMS para proteção autônoma contra ransomware.

Tópicos

- Habilitando a proteção autônoma contra ransomware
- Respondendo aos alertas da Autonomous Ransomware Protection
- Entendendo os alertas do EMS para proteção autônoma contra ransomware

Habilitando a proteção autônoma contra ransomware

Os procedimentos a seguir explicam como usar o ONTAP CLI para ativar a Proteção Autônoma contra Ransomware (ARP) no modo de aprendizado e no modo ativo, bem como verificar se o ARP está ativado. Para obter mais informações sobre o ARP, consulteComo funciona o ARP.

Habilitando o ARP no modo de aprendizado

Para habilitar o ARP no modo de aprendizado em um volume existente usando o ONTAP CLI

- Execute o seguinte comando: Substitua *vol_name* e *svm_name* pelas próprias informações.

  ```
  security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
  ```

  Para obter mais informações sobre esse comando, consulte `security anti-ransomware volume dry-run`no NetApp centro de documentação.

  > **Note**
  >
  > O modo de aprendizado só se aplica a dados recém-gravados. Os dados existentes não são digitalizados nem analisados. Os comportamentos normais do tráfego de dados são determinados com base nos novos dados gravados após a ativação do ARP no volume.

Para habilitar o ARP no modo de aprendizado em um novo volume usando o ONTAP CLI

- Execute o seguinte comando: Substitua *vol_namesvm_name*,*size*,, e */path_name* por suas informações.

  ```
  volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size size -
  anti-ransomware-state dry-run -junction-path /path_name
  ```

  Para obter mais informações sobre esse comando, consulte `volume create`no NetApp centro de documentação.

Ativando o ARP no modo ativo

Para habilitar o ARP no modo ativo em um volume existente usando o ONTAP CLI

- Execute o seguinte comando: Substitua *vol_name* e *svm_name* pelas próprias informações.

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

Para obter mais informações sobre esse comando, consulte security anti-ransomware volume enableno NetApp centro de documentação.

> **Note**
>
> Recomendamos manter um volume no modo de aprendizado por no mínimo 30 dias antes de converter para o modo ativo. O ARP determina automaticamente o período de aprendizado ideal e muda do modo de aprendizado quando estiver pronto. Esse processo pode ocorrer em menos de 30 dias.

Ativando o ARP por padrão no nível do SVM

Para habilitar o ARP por padrão em um SVM existente usando o ONTAP CLI

- Execute o seguinte comando: *svm_name*Substitua por suas próprias informações.

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

Para obter mais informações sobre esse comando, consulte vserver modifyno NetApp centro de documentação.

Verificando o status do ARP

Para verificar o status do ARP usando o ONTAP CLI

- Execute o seguinte comando:

```
security anti-ransomware volume show
```

Para obter mais informações sobre esse comando, consulte `security anti-ransomware volume show`no NetApp centro de documentação.

Você pode suspender temporariamente (e depois retomar) o ARP se estiver prevendo eventos de carga de trabalho pesada. Para obter mais informações, consulte Pause ONTAP Autonomous Ransomware Protection para excluir eventos de carga de trabalho da análise no NetApp Centro de Documentação.

Respondendo aos alertas da Autonomous Ransomware Protection

Os procedimentos a seguir explicam como usar o ONTAP CLI para visualizar alertas do Autonomous Ransomware Protection (ARP), gerar relatórios de ataque e agir com base nos relatórios. Para obter mais informações sobre como o ARP detecta e responde aos ataques, consulte e. O que o ARP procura Como responder a um ataque suspeito com o ARP

Visualizando alertas ARP

Para visualizar um alerta ARP em um volume usando o ONTAP CLI

- Execute o seguinte comando: Substitua *svm_name* e *vol_name* pelas próprias informações.

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

Depois de executar o comando, você verá uma saída semelhante ao exemplo a seguir:

```
Vserver Name: fsx
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

Para obter mais informações sobre esse comando, consulte `security anti-ransomware volume show`no NetApp centro de documentação.

Gerando relatórios ARP

Para gerar relatórios ARP usando o ONTAP CLI

- Execute o seguinte comando: Substitua *vol_name* e */file_location/* pelas próprias informações. Depois de gerar o relatório, você pode visualizá-lo em um sistema cliente.

```
security anti-ransomware volume attack generate-report -volume vol_name -dest-
path /file_location/
```

  Para obter mais informações sobre esse comando, consulte security anti-ransomware volume attack generate-reportno NetApp centro de documentação.

Agindo com base nos relatórios do ARP

Para agir em relação a um ataque falso positivo de um relatório ARP usando o ONTAP CLI

- Execute o seguinte comando: Substitua *svm_namevol_name*,, e *[extension identifiers]* por suas próprias informações.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive true
```

  Para obter mais informações sobre esse comando, consulte security anti-ransomware volume attack clear-suspectno NetApp centro de documentação.

> **Note**
>
> Quando você marca um alerta como falso positivo, ele atualiza o perfil do ransomware. Depois de fazer isso, você não receberá um alerta sobre esse cenário específico novamente.

Para agir em relação a um possível ataque a partir de um relatório ARP usando o ONTAP CLI

- Execute o seguinte comando: Substitua *svm_namevol_name*,, e *[extension identifiers]* por suas próprias informações.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive false
```

Para obter mais informações sobre esse comando, consulte `security anti-ransomware volume attack clear-suspect`no NetApp centro de documentação.

Entendendo os alertas do EMS para proteção autônoma contra ransomware

Você pode usar: NetApp ONTAP's Sistema de gerenciamento de eventos (EMS) para monitorar eventos relacionados ao ARP, incluindo possíveis ataques. Para obter mais informações sobre o ARP e como ele detecta ataques, consulte e. Como funciona o ARP O que o ARP procura

A tabela a seguir contém todos os alertas relacionados ao ARP. Para obter mais informações sobre o EMS, consulteMonitoramento FSx de eventos do ONTAP EMS.

Nome da mensagem EMS	Descrição da mensagem EMS
`arw.analytics.ext.report`	Essa mensagem ocorre quando a análise anti-ransomware gera ou atualiza o relatório de extensões de arquivo suspeitas de um volume.
`arw.analytics.high.entropy`	Essa mensagem ocorre quando o número de mensagens de registro de dados de alta entropia (relacionadas à detecção e análise de ransomware) ultrapassa o limite predefinido para um volume.
`arw.analytics.probability`	Essa mensagem ocorre quando a probabili dade de um ataque anti-ransomware muda de `low` para `high` em um volume.
`arw.analytics.report`	Essa mensagem ocorre quando um relatório analítico anti-ransomware é gerado ou atualizado para um volume.

Nome da mensagem EMS	Descrição da mensagem EMS
`arw.analytics.suspects`	Essa mensagem ocorre quando uma lista de suspeitos gerada pela análise anti-ransomware cresce até um ponto em que é necessária uma investigação mais aprofundada.
`arw.auto.switch.enabled`	Essa mensagem ocorre quando o anti-rans omware é automaticamente alternado do modo de aprendizado para ativado após várias condições terem sido satisfeitas, como período de aprendizado, criação de arquivos, gravação de arquivos e atividades de descoberta de extensões de arquivos.
`arw.new.file.extn.seen`	Essa mensagem ocorre quando uma nova extensão de arquivo é observada em um volume habilitado para anti-ransomware. Seu objetivo é notificar prontamente o usuário sobre a extensão observada, o que permite uma investigação oportuna.
`arw.snapshot.created`	Essa mensagem ocorre quando um novo instantâneo ARP é criado em um volume habilitado para anti-ransomware. Além disso, ele fornece informações sobre o motivo pelo qual o instantâneo foi criado.
`arw.volume.state`	Essa mensagem ocorre quando o estado anti-ransomware de um volume é alterado.
`arw.vserver.state`	Essa mensagem ocorre quando o estado anti-ransomware de um SVM é alterado.

Protegendo seus dados com SnapLock

SnapLock é um recurso que permite proteger seus arquivos fazendo a transição para o estado WORM (Write Once, Read Many), o que impede modificações ou exclusões por um período de retenção especificado. Você pode usar: SnapLock para atender à conformidade regulatória, proteger dados essenciais para os negócios contra ataques de ransomware e fornecer uma camada adicional de proteção para seus dados contra alteração ou exclusão.

O Amazon FSx for NetApp ONTAP oferece suporte aos modos de retenção de conformidade e corporativos com SnapLock. Para obter mais informações, consulte Noções básicas SnapLock Compliance Noções básicas SnapLock Enterprise e.

Você pode criar SnapLock volumes ativados FSx para sistemas de arquivos ONTAP criados em ou após 13 de julho de 2023. Os sistemas de arquivos existentes obterão SnapLock suporte durante uma próxima janela de manutenção semanal.

Tópicos

- Como SnapLock funciona
- Noções básicas SnapLock Compliance
- Noções básicas SnapLock Enterprise
- Entendendo o SnapLock período de retenção
- Confirmar arquivos para o estado WORM

Como SnapLock funciona

SnapLock pode ajudá-lo a atender às finalidades regulatórias e de controle, impedindo que seus arquivos sejam excluídos, alterados ou renomeados. Quando você cria um SnapLock volume, você compromete seus arquivos para gravar uma vez, ler muitos (WORM) e define períodos de retenção para os dados. Seus arquivos podem ser armazenados em um estado não apagável e não gravável por um período designado ou indefinidamente.

> **Important**
>
> Você deve especificar se um volume usará SnapLock configurações no momento da criação. Um não-SnapLock o volume não pode ser convertido em um SnapLock volume após a criação.

Modos de retenção

SnapLock tem dois modos de retenção: Compliance e Enterprise. O Amazon FSx for NetApp ONTAP oferece suporte a ambos. Eles têm casos de uso distintos e alguns dos recursos são diferentes, mas ambos protegem seus dados contra modificação ou exclusão usando o modelo WORM. A tabela a seguir explica algumas das semelhanças e diferenças entre esses modos de retenção.

SnapLock recurso	Noções básicas SnapLock Compliance	Noções básicas SnapLock Enterprise
Descrição	Os arquivos que recebem a transição para o WORM em um volume Compliance não podem ser excluídos até que seus períodos de retenção expirem.	Os arquivos que recebem a transição para o WORM em um volume Enterprise podem ser excluídos por usuários autorizados antes que seus períodos de retenção expirem usando a exclusão privilegi ada.
Casos de uso	• Tratar de exigência s governamentais ou específicos do setor, como a Norma 17a-4(f) da SEC, a Norma 4511 da FINRA e a Regulamentação 1.31 da CFTC. • Proteger-se contra ataques de ransomware.	• Promover a integridade dos dados e a conformidade interna de uma organização. • Para testar as configura ções de retenção antes de usar SnapLock Conformid ade.
Confirmação automática	Sim	Sim
Retenção baseada em eventos (EBR)[1]	Sim	Sim
Retenções jurídicas[1]	Sim	Não
Usando a exclusão privilegi ada	Não	Sim

SnapLock recurso	Noções básicas SnapLock Compliance	Noções básicas SnapLock Enterprise
Modo de acréscimo de volume	Sim	Sim
SnapLock volumes de registros de auditoria	Sim	Sim

> **Note**
>
> [1] As operações de EBR e Legal Hold são suportadas no ONTAP CLI e API REST.

> **Note**
>
> FSx for ONTAP suporta a classificação de dados em camadas para o pool de capacidade em todos SnapLock volumes, independentemente do SnapLock type. Para obter mais informações, consulte Divisão de dados em níveis no volume.

SnapLock Administrador

Você deve ter... SnapLock privilégios de administrador para realizar determinadas ações em SnapLock volumes. SnapLock os privilégios de administrador são definidos na `vsadmin-snaplock` função no ONTAP CLI. Você deve ser administrador de cluster para criar uma conta de administrador de máquina virtual de armazenamento (SVM) com o SnapLock função de administrador.

Você pode realizar as seguintes ações com a `vsadmin-snaplock` função no ONTAP CLI:

- Gerenciar sua própria conta de usuário, senha local e informações importantes
- Gerenciar volumes, exceto volumes móveis
- Gerenciar cotas, qtrees, cópias de snapshots e arquivos
- Executar SnapLock ações, incluindo exclusão privilegiada e retenção legal
- Configurar os protocolos Network File System (NFS) e Server Message Block (SMB)
- Configurar os serviços do Sistema de Nomes de Domínio (DNS), do Lightweight Directory Access Protocol (LDAP) e do Network Information Service (NIS)

- Monitorar trabalhos

O procedimento a seguir detalha como criar um SnapLock administrador no ONTAP CLI. É necessário fazer login como administrador de cluster em uma conexão segura, como o protocolo Secure Shell (SSH), para realizar essa tarefa.

Para criar uma conta de administrador do SVM com a função vsadmin-snaplock no ONTAP CLI

- Execute o seguinte comando: Substitua *SVM_name* e *SnapLockAdmin* pelas próprias informações.

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

Para obter mais informações, consulte Usuários e perfis do ONTAP.

SnapLock volumes de registros de auditoria

A SnapLock o volume do registro de auditoria contém SnapLock registros de auditoria, que contêm registros de data e hora de eventos, como quando um SnapLock O administrador foi criado, quando operações de exclusão privilegiadas foram executadas ou quando uma retenção legal foi colocada nos arquivos. A ferramenta SnapLock o volume do registro de auditoria é um registro não apagável de eventos.

Você deve criar um SnapLock volume de registros de auditoria no mesmo SVM do SnapLock volume para as seguintes ações:

- Para ativar ou desativar a exclusão privilegiada em um SnapLock Volume corporativo.
- Para aplicar a retenção legal em um arquivo em um SnapLock Volume de conformidade.

> ⚠ Warning
>
> - O período mínimo de retenção para um SnapLock o volume do registro de auditoria é de seis meses. Até que esse período de retenção expire, o SnapLock o volume do log de auditoria e o SVM e o sistema de arquivos associados a ele não podem ser excluídos, mesmo que o volume tenha sido criado no SnapLock Modo empresarial.

- Se um arquivo for excluído usando a exclusão privilegiada e seu período de retenção for maior que o período de retenção do volume, o volume do log de auditoria herdará o período de retenção do arquivo. Por exemplo, se um arquivo com um período de retenção de dez meses for excluído usando a exclusão privilegiada e o período de retenção do volume do log de auditoria for de seis meses, o período de retenção do volume do log de auditoria será estendido para dez meses.

Você pode ter apenas um ativo SnapLock volume de registros de auditoria em uma SVM, mas ele pode ser compartilhado por vários SnapLock volumes no SVM. Para montar um SnapLock volume de log de auditoria com sucesso, defina o caminho de junção como`/snaplock_audit_log`. Nenhum outro volume pode usar esse caminho da junção, incluindo volumes que não sejam do log de auditoria.

Você pode encontrar SnapLock registros de auditoria no `/snaplock_log` diretório abaixo da raiz do volume de registros de auditoria. As operações de exclusão privilegiadas são registradas em log no subdiretório `privdel_log`. As operações de início e término da retenção jurídica são registradas em log em `/snaplock_log/legal_hold_logs/`. Todos os outros log são armazenados no subdiretório `system_log`.

Você pode criar um SnapLock volume de registros de auditoria com o FSx console da Amazon AWS CLI, o, a FSx API da Amazon e o ONTAP CLI e API REST.

> **Note**
>
> Um volume de proteção de dados (DP) não pode ser usado como SnapLock volume do registro de auditoria.

Para ativar o SnapLock volume de log de auditoria com a FSx API da Amazon, use `AuditLogVolume` no `CreateSnaplockConfiguration`. No FSx console da Amazon, em Volume do log de auditoria, escolha Ativado. Certifique-se de que o Caminho da junção esteja definido como `/snaplock_audit_log`.

Acessando seus dados em um SnapLock volume

Você pode usar protocolos de arquivos abertos, como NFS e SMB, para acessar seus dados em um SnapLock volume. Não há impacto no desempenho ao gravar dados em um SnapLock volume ou da leitura de dados protegidos pelo WORM.

Você pode copiar arquivos entre SnapLock volumes com NFS e SMB, mas eles não manterão suas propriedades WORM no destino SnapLock volume. Você deve reconfirmar os arquivos copiados para o WORM a fim de evitar que sejam modificados ou excluídos. Para obter mais informações, consulte Confirmar arquivos para o estado WORM.

Você também pode replicar SnapLock dados com SnapMirror, mas os volumes de origem e destino devem ser SnapLock volumes com o mesmo modo de retenção (por exemplo, ambos devem ser Compliance ou Enterprise).

Noções básicas SnapLock Compliance

Esta seção descreve casos de uso e considerações para o SnapLock Modo de retenção de conformidade.

Você pode escolher o modo de retenção Compliance para os casos de uso a seguir.

- Você pode usar: SnapLock Conformidade para atender a mandatos governamentais ou específicos do setor, como a Regra 17a-4 (f) da SEC, a Regra 4511 da FINRA e a Regulamentação 1.31 da CFTC. SnapLock A conformidade do NetApp ONTAP na Amazon FSx foi avaliada para esses mandatos e regulamentações por Cohasset Associates. Para obter mais informações, consulte o Relatório de avaliação de conformidade da Amazon FSx para NetApp ONTAP.
- Você pode usar: SnapLock Conformidade para complementar ou aprimorar uma estratégia abrangente de proteção de dados para combater ataques de ransomware.

Aqui estão alguns itens importantes a serem considerados sobre o SnapLock Modo de retenção de conformidade.

- Depois que um arquivo é transferido para o estado Write Once, Read Many (WORM) em um SnapLock Volume de conformidade, ele não pode ser excluído antes que seu período de retenção expire por qualquer usuário.
- A SnapLock O volume de conformidade só pode ser excluído quando os períodos de retenção de todos os arquivos WORM no volume expirarem e os arquivos WORM tiverem sido excluídos do volume.
- Você não pode renomear um SnapLock Volume de conformidade após a criação.
- Você pode usar SnapMirror para replicar arquivos WORM, mas o volume de origem e o volume de destino devem ter o mesmo modo de retenção (por exemplo, ambos devem estar em conformidade).

- A SnapLock O volume de conformidade não pode ser convertido em SnapLock Volume corporativo e vice-versa.

Noções básicas SnapLock Enterprise

Esta seção descreve casos de uso e considerações para o SnapLock Modo de retenção empresarial.

Você pode escolher o SnapLock Modo de retenção empresarial para os seguintes casos de uso.

- Você pode usar: SnapLock Enterprise autorizará somente usuários específicos a excluir arquivos.
- Você pode usar: SnapLock Enterprise para aprimorar a integridade dos dados e a conformidade interna da sua organização.
- Você pode usar: SnapLock Empresa testará as configurações de retenção antes de usar SnapLock Conformidade.

Aqui estão alguns itens importantes a serem considerados sobre o SnapLock Modo de retenção empresarial.

- Você pode usar: SnapMirror para replicar arquivos WORM, mas o volume de origem e o volume de destino devem ter o mesmo modo de retenção (por exemplo, ambos devem ser Enterprise).
- A SnapLock o volume não pode ser convertido de Enterprise para Compliance ou de Compliance para Enterprise.
- SnapLock O Enterprise não oferece suporte ao Legal Hold.

Usando a exclusão privilegiada

Uma das principais diferenças entre SnapLock Empresa e SnapLock Conformidade é que um SnapLock o administrador pode ativar a exclusão privilegiada em um SnapLock Volume corporativo para permitir que um arquivo seja excluído antes que o período de retenção do arquivo expire. A ferramenta SnapLock administrador é o único usuário que pode excluir arquivos de um SnapLock Volume corporativo que tem políticas de retenção ativas inseridas nele. Para obter mais informações, consulte SnapLock Administrador.

Você pode ativar ou desativar a exclusão privilegiada com o FSx console da Amazon AWS CLI, a FSx API da Amazon e a ONTAP CLI e API REST. Para ativar a exclusão privilegiada, você deve primeiro criar um SnapLock volume de registros de auditoria no mesmo SVM do SnapLock volume. Para obter mais informações, consulte SnapLock volumes de registros de auditoria.

Para ativar a exclusão privilegiada com a FSx API da Amazon, use `PrivilegedDelete` no `CreateSnaplockConfiguration`. No FSx console da Amazon, em Privileged Delete, escolha Enabled.

> **Note**
>
> Não é possível emitir um comando de exclusão privilegiada para excluir um arquivo de gravação única e várias leituras (WORM) que tenha um período de retenção expirado. Você pode executar uma operação de exclusão normal após o período de retenção expirar.

Você pode optar por desativar a exclusão privilegiada permanentemente, mas essa ação é irreversível. Se a exclusão privilegiada estiver permanentemente desativada, você não precisará ter um SnapLock volume de registros de auditoria associado ao SnapLock Volume corporativo.

Para desativar permanentemente a exclusão privilegiada com a FSx API da Amazon, use `PrivilegedDelete` no `CreateSnaplockConfiguration`. No FSx console da Amazon, em Privileged Delete, escolha Permanentemente desativado.

Ignorando SnapLock Modo empresarial

Se você estiver usando o FSx console da Amazon ou a FSx API da Amazon, deverá ter a `fsx:BypassSnapLockEnterpriseRetention` permissão do IAM para excluir um SnapLock Volume corporativo que contém arquivos WORM com políticas de retenção ativas.

Para obter mais informações, consulte Excluindo SnapLock volumes.

Entendendo o SnapLock período de retenção

Quando você cria um SnapLock volume, você pode definir um período de retenção padrão para o volume ou definir o período de retenção para gravar uma vez, ler muitos arquivos (WORM) explicitamente. Durante o período de retenção, não é possível excluir nem modificar arquivos protegidos por WORM. O período de retenção é usado para calcular o tempo de retenção. Por exemplo, se fizer a transição de um arquivo para o WORM em 14 de julho de 2023 à meia-noite e definir o período de retenção como cinco anos, o tempo de retenção será até 14 de julho de 2028 à meia-noite.

Para obter mais informações sobre o WORM, consulte Confirmar arquivos para o estado WORM.

Políticas de período de retenção

O período de retenção é determinado pelos valores atribuídos aos seguintes parâmetros:

- Retenção padrão: o período de retenção padrão atribuído a um arquivo WORM se você não fornecer um período de retenção explícito para ele.
- Retenção mínima: o período de retenção mais curto que pode ser atribuído a um arquivo WORM.
- Retenção máxima: o período de retenção mais longo que pode ser atribuído a um arquivo WORM.

> **Note**
>
> Mesmo após o período de retenção expirar, não será possível modificar um arquivo WORM. Você só poderá excluí-lo ou definir um novo período de retenção para ativar a proteção WORM novamente.

Você pode especificar o período de retenção usando várias unidades de tempo diferentes. A tabela a seguir lista os intervalos específicos com suporte.

Tipo	Valor	Observações
Segundos	0 a 65.535	
Minutos	0 a 65.535	
Horas	0 a 24	
Dias	0 a 365	
Meses	0 a 12	
Anos	0 a 100	
Infinito	-	Retém os arquivos para sempre.

Tipo	Valor	Observações
		Disponível para Retenção padrão, Retenção máxima e Retenção mínima.
Não especificado 1	-	Retém os arquivos até que você defina um período de retenção. Disponível somente para Retenção padrão.

> **Note**
>
> [1] Quando você faz a transição de arquivos para o WORM com um período de retenção não especificado, eles recebem o período mínimo de retenção configurado para o SnapLock volume. Ao fazer a transição dos arquivos protegidos por WORM para um tempo de retenção absoluto, o novo período de retenção deve ser maior do que o período mínimo definido anteriormente nos arquivos.

Período de retenção expirado

Após o período de retenção de um arquivo WORM expirar, você poderá excluir o arquivo ou definir um novo período de retenção para ativar a proteção WORM novamente. Os arquivos WORM não são excluídos automaticamente após o período de retenção expirar. Ainda assim, não é possível modificar o conteúdo de um arquivo WORM, mesmo após o período de retenção expirar.

Definindo o período de retenção de um SnapLock volume

Você pode definir o período de retenção de um SnapLock volume com o FSx console da Amazon, o AWS CLI, a FSx API da Amazon e o ONTAP CLI e API REST.

Para definir o período de retenção com a FSx API da Amazon, use a `SnaplockRetentionPeriod`configuração. No FSx console da Amazon, para Período de retenção, insira valores para Retenção padrão, Retenção mínima e Retenção máxima. Em seguida, escolha uma Unidade correspondente para cada uma.

Confirmar arquivos para o estado WORM

Esta seção explica como fazer a transição dos seus arquivos para um estado de gravação única e várias leituras (WORM). Também será discutido o modo de acréscimo de volume, que é uma forma de gravar dados de forma incremental em arquivos protegidos por WORM.

Confirmação automática

Você pode usar a confirmação automática para fazer a transição de arquivos para o WORM se eles não tiverem sido modificados durante um período especificado por você. Você pode ativar a confirmação automática com o FSx console da Amazon, o AWS CLI, a FSx API da Amazon e o ONTAP CLI e API REST.

Você pode especificar um período de confirmação automática entre cinco minutos e dez anos. A tabela a seguir lista os intervalos específicos com suporte.

Unidade	Valor
Minutos	5 a 65.535
Horas	1 a 65,535
Dias	1 a 3.650
Meses	1 a 120
Anos	1 a 10

Para ativar a confirmação automática com a FSx API da Amazon, use `AutocommitPeriod` no `CreateSnaplockConfiguration`. No FSx console da Amazon, em Autocommit, escolha Enabled. Em seguida, em Período de confirmação automática, insira um valor e escolha uma Unidade de confirmação automática correspondente.

Você pode especificar um valor entre cinco minutos e dez anos.

Modo de acréscimo de volume

Não é possível modificar dados existentes em um arquivo protegido por WORM. No entanto, SnapLock permite que você mantenha a proteção dos dados existentes usando arquivos anexáveis ao WORM. Por exemplo, você pode gerar arquivos de log ou preservar dados de streaming de áudio

ou vídeo enquanto grava dados neles de forma incremental. Você pode ativar ou desativar o modo de acréscimo de volume com o FSx console da Amazon, o, AWS CLI a API da Amazon FSx e o ONTAP CLI e API REST.

Requisitos para atualizar o modo de acréscimo de volume

- A ferramenta SnapLock o volume deve estar desmontado.
- A ferramenta SnapLock o volume deve estar vazio de cópias instantâneas e dados do usuário.

Para ativar o modo de acréscimo de volume com a FSx API da Amazon, use no. `VolumeAppendModeEnabled` `CreateSnaplockConfiguration` No FSx console da Amazon, no modo de acréscimo de volume, escolha Ativado.

Retenção baseada em eventos (EBR)

Você pode usar a retenção baseada em eventos (EBR) para criar políticas personalizadas com períodos de retenção associados. Por exemplo, você pode fazer a transição de todos os arquivos em um caminho especificado para o WORM e definir o período de retenção para um ano com os comandos `snaplock event-retention policy create` e `snaplock event-retention apply`. Ao usar a EBR, é necessário especificar um volume, um diretório ou um arquivo. O período de retenção selecionado ao criar a política de EBR é aplicado a todos os arquivos no caminho especificado.

O EBR é apoiado pelo ONTAP CLI e API REST.

> **Note**
>
> ONTAP não suporta EBR com FlexGroup volumes.

Os procedimentos a seguir explicam como criar, aplicar, modificar e excluir uma política de EBR. Você deve ser um SnapLock administrador (tem a `vsadmin-snaplock` função) para concluir essas tarefas no ONTAP CLI. Para obter mais informações, consulte SnapLock Administrador.

Criando uma política de EBR no ONTAP CLI

Para criar uma política de EBR no ONTAP CLI

- Execute o seguinte comando: Substitua *`p1`* e *`"10 years"`* pelas próprias informações.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

Aplicando uma política de EBR no ONTAP CLI

Para aplicar uma política de EBR no ONTAP CLI

- Execute o seguinte comando: Substitua *p1* e *slc* pelas próprias informações. Você pode adicionar um caminho após a barra (/) se quiser especificar um determinado caminho para a política de EBR. Caso contrário, esse comando aplicará a política de EBR a todos os arquivos no volume.

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

Modificando uma política de EBR no ONTAP CLI

Para modificar uma política de EBR no ONTAP CLI

- Execute o seguinte comando: Substitua *p1* e *"5 years"* pelas próprias informações.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

Excluindo uma política de EBR no ONTAP CLI

Para excluir uma política de EBR no ONTAP CLI

- Execute o seguinte comando: *p1*Substitua por suas próprias informações.

```
vs1::> snaplock event-retention policy delete -name p1
```

Comandos relacionados no NetApp Centro de documentação:

- snaplock event-retention abort
- snaplock event-retention show-vservers
- snaplock event-retention show
- snaplock event-retention policy show

Retenções jurídicas

É possível reter arquivos WORM por um período indefinido usando a retenção jurídica. Geralmente, a retenção jurídica é usada para fins de litígio. Um arquivo WORM sujeito a uma retenção jurídica não pode ser excluído até que a restrição legal seja suspensa.

O Legal Hold é apoiado pelo ONTAP CLI e API REST.

> **Note**
>
> ONTAP não suporta Legal Hold com FlexGroup volumes.

Os procedimentos a seguir explicam como iniciar e encerrar uma retenção jurídica. Você deve ser um SnapLock administrador (tem a `vsadmin-snaplock` função) para concluir essas tarefas no ONTAP CLI. Para obter mais informações, consulte SnapLock Administrador.

Iniciando uma retenção legal em um arquivo em um SnapLock Volume de conformidade com o ONTAP CLI

Para iniciar uma retenção legal em um arquivo em um SnapLock Volume de conformidade com o ONTAP CLI

- Execute o seguinte comando: Substitua *`litigation1slc_vol1`*, e *`file1`* por suas próprias informações.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Iniciando uma retenção legal em todos os arquivos em um SnapLock Volume de conformidade com o ONTAP CLI

Para iniciar uma retenção legal em todos os arquivos em um SnapLock Volume de conformidade com o ONTAP CLI

- Execute o seguinte comando: Substitua *`litigation1`* e *`slc_vol1`* pelas próprias informações.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /
```

Encerrando uma retenção legal em um arquivo em um SnapLock Volume de conformidade com o ONTAP CLI

Para encerrar uma retenção legal em um arquivo em um SnapLock Volume de conformidade com o ONTAP CLI

- Execute o seguinte comando: Substitua *litigation1slc_vol1*, e *file1* por suas próprias informações.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

> **Note**
>
> Recomendamos que monitore o `-operation-status` com o comando `snaplock legal-hold show` ao emitir uma retenção jurídica para garantir que ela não falhe.

Encerrando uma retenção legal em todos os arquivos em um SnapLock Volume de conformidade com o ONTAP CLI

Para encerrar uma retenção legal em todos os arquivos em um SnapLock Volume de conformidade com o ONTAP CLI

- Execute o seguinte comando: Substitua *litigation1* e *slc_vol1* pelas próprias informações.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /
```

> **Note**
>
> Recomendamos que monitore o `-operation-status` com o comando `snaplock legal-hold show` ao emitir uma retenção jurídica para garantir que ela não falhe.

Comandos relacionados no NetApp Centro de documentação:

- snaplock legal-hold abort

- snaplock legal-hold dump-files
- snaplock legal-hold dump-litigations
- snaplock legal-hold show

Replicando seus dados com FlexCache

FlexCacheé um recurso de cache NetApp ONTAP's remoto que aproxima os conjuntos de dados dos clientes, melhorando o desempenho do acesso e reduzindo os custos. Ele simplifica a distribuição de arquivos e reduz os custos de WAN. Quando você cria um FlexCache volume, ele inicialmente copia somente os metadados do sistema de arquivos de origem. Essa abordagem é mais rápida e mais eficiente em termos de espaço do que uma cópia completa dos dados, consumindo apenas uma fração da capacidade de armazenamento.

Como a FlexCache funciona

Um FlexCache volume é um cache pouco preenchido que fornece acesso aos dados armazenados em um volume de origem. O cache pode estar localizado em um sistema de arquivos diferente, opcionalmente remoto. Em vez de copiar todos os dados do volume de origem, FlexCache copia os dados somente quando necessário. FlexCacheos volumes são mais adequados para fluxos de trabalho de leitura intensiva com alterações de dados pouco frequentes, pois qualquer alteração nos dados de origem exige que o cache seja atualizado.

Você pode usar FlexCache com FSx for ONTAP nas seguintes configurações:

Volume de origem	FlexCache volume
No local NetApp ONTAP	FSx para ONTAP
FSx para ONTAP	No local NetApp ONTAP
FSx para ONTAP	FSx para ONTAP

FlexCachemodos de gravação

FlexCacheos volumes suportam dois modos de operação para operações de gravação: modo de gravação e modo de gravação.

No modo de gravação, que é o modo padrão, as gravações são encaminhadas do cache para o volume de origem. A operação de gravação não é confirmada para o cliente até que os dados sejam confirmados para armazenamento no volume de origem e a origem reconheça a gravação no cache. Como cada gravação deve atravessar a rede entre o cache e a origem, esse modo tem maior latência do que o modo de gravação.

No modo write-back, introduzido na versão ONTAP 9.15.1, as gravações são confirmadas no armazenamento no local do cache e imediatamente confirmadas para o cliente. Os dados são então gravados de forma assíncrona no volume de origem. Esse modo permite que as gravações sejam executadas em velocidades quase locais, o que pode melhorar significativamente o desempenho de cargas de trabalho distribuídas.

Use o modo write-back para cargas de trabalho com muita gravação que exigem gravações em cache de baixa latência. Use o modo de gravação para cargas de trabalho de leitura intensa que não são sensíveis à latência ou quando seu sistema de arquivos de origem tem mais de 10 volumes de origem. FlexCache

FlexCachevisão geral da criação de volume

A criação FlexCache de um volume consiste nas seguintes etapas:

- Reúna interfaces lógicas de origem e destino (LIFs)
- Estabeleça o emparelhamento de clusters entre os sistemas de arquivos de origem e cache
- Crie uma relação de emparelhamento de máquina virtual de armazenamento (SVM)
- Crie o FlexCache volume e selecione um modo de gravação
- Monte o FlexCache volume em seus clientes

Para obter instruções detalhadas, consulte Criação de um FlexCache.

Criação de um FlexCache

Usando os procedimentos a seguir, você criará um FlexCache volume em um sistema de arquivos Amazon FSx for NetApp ONTAP, que é apoiado por um volume de origem localizado em um cluster localNetApp ONTAP.

Usar a CLI do ONTAP

Você usará a ONTAP CLI para criar e gerenciar uma FlexCache configuração no seu sistema de arquivos FSx for ONTAP.

Os comandos nesses procedimentos usam os seguintes aliases para o cluster, SVM e volume:

- `Cache_ID`— o ID do cluster de cache (no formato FSx IDABCDEF1234567890a)
- `Origin_ID`— o ID do cluster de origem
- `CacheSVM`— o nome do cache SVM
- `OriginSVM`— o nome SVM de origem
- `OriginVol`— o nome do volume de origem
- `CacheVol`— o nome FlexCache do volume

Os procedimentos nesta seção usam os seguintes comandos da NetApp ONTAP CLI.

- `network interfaces show`
- Comandos `cluster peer`
- `volume flexcache create`

Pré-requisitos

Antes de começar a usar os procedimentos nas seções a seguir, verifique se você atendeu aos seguintes pré-requisitos:

- Os sistemas de arquivos de origem e destino estão conectados na mesma VPC ou em redes que são emparelhadas usando Amazon VPC,,, ou. AWS Transit Gateway AWS Direct Connect AWS VPN Para obter mais informações, consulte O que é Acessando dados de dentro do Nuvem AWS emparelhamento de VPC? no Guia de emparelhamento do Amazon VPC.
- O grupo de segurança VPC FSx para o sistema de arquivos ONTAP tem regras de entrada e saída que permitem ICMP e TCP nas portas 11104 e 11105 para seus endpoints entre clusters (). LIFs
- Você criou um destino FSx para o sistema de arquivos ONTAP com um SVM, mas não criou o volume que será usado como. FlexCache Para obter mais informações, consulte Criar sistemas de arquivos.

Registre a origem e o destino entre clusters LIFs

1. FSx Para o sistema de arquivos for ONTAP que é o cluster de destino:

   a. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.

b. Escolha Sistemas de arquivos e, em seguida, escolha o sistema FSx de arquivos ONTAP que é o cluster de destino para abrir a página de detalhes do sistema de arquivos.

c. Em Administração, localize o endpoint entre clusters - endereços IP e registre o valor.

> **Note**
>
> Para sistemas de arquivos escaláveis, há dois endereços IP de endpoint entre clusters para cada par de alta disponibilidade (HA).

2. Para o cluster de origem local, recupere os endereços IP LIF entre clusters usando o seguinte comando da CLI: ONTAP

```
Origin::> network interface show -role intercluster
Logical                         Network
Vserver     Interface  Status   Address/Mask
----------- ---------- -------  ------------
OriginSVM
            inter_1     up/up   10.0.0.36/24
            inter_2     up/up   10.0.1.69/24
```

3. Salve `inter_1` os `inter_2` IP endereços e. Eles são referenciados no `OriginSVM` alias como `origin_inter_1` e `origin_inter_2` e no `CacheSVM` alias como e. `cache_inter_1` `cache_inter_2`

Estabeleça o emparelhamento de clusters entre a origem e o cache

Estabeleça uma relação de pares de cluster no Source cluster Cache e usando o comando cluster peer createONTAPCLI. Você fornecerá os endereços IP entre clusters que salvou anteriormente no Registre a origem e o destino entre clusters LIFs procedimento. Quando solicitado, você deverá criar um *`cluster-peer-passphrase`* que precisará inserir ao estabelecer o peering de cluster no Origin cluster.

1. Configure o emparelhamento de `Cache` clusters no cluster (seu FSx para o sistema de arquivos ONTAP).

   a. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a

seguir. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

b. Use o comando a seguir e registre a senha que você criou. Para sistemas de arquivos escaláveis, forneça os endereços `inter_2` IP `inter_1` e para cada par de HA.

```
FSx-Cache::> cluster peer create -address-family ipv4 -peer-
addrs origin_inter_1,origin_inter_2

Enter the passphrase: cluster-peer-passphrase
Confirm the passphrase: cluster-peer-passphrase
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. Use o comando a seguir para configurar o emparelhamento de clusters no cluster `source` (local). Você precisará inserir a senha criada na etapa anterior para se autenticar. Para sistemas de arquivos escaláveis, você precisará fornecer o endereço IP entre clusters para cada par de HA.

```
Origin::> cluster peer create -address-family ipv4 -peer-
addrs cache_inter_1,cache_inter_2

Enter the passphrase: cluster-peer-passphrase
Confirm the passphrase: cluster-peer-passphrase
```

3. No `source` cluster, verifique se o emparelhamento de clusters foi configurado com êxito usando o comando a seguir. Na saída, `Availability` deve ser definida como `Available`.

```
Origin::> cluster peer show

Peer Cluster Name     Availability    Authentication
-------------------   -------------   --------------
Cache_ID              Available       ok
```

Se a saída não aparecer`Available`, repita as etapas anteriores nos `cache` clusters `source` e.

Configurar o emparelhamento da máquina virtual de armazenamento (SVM)

Depois de estabelecer o emparelhamento de clusters com êxito, a próxima etapa é criar um relacionamento de emparelhamento de SVM no cluster de cache (Cache) usando o comando. vserver peer Os aliases adicionais usados no procedimento a seguir são os seguintes:

- *`CacheLocalName`*— o nome usado para identificar o `cache` SVM ao configurar o emparelhamento de SVM no SVM. `origin`
- *`OriginLocalName`*— o nome usado para identificar o `origin` SVM ao configurar o emparelhamento de SVM no SVM. `cache`

1. No `cache` SVM, use o comando a seguir para criar um relacionamento de emparelhamento do SVM.

```
FSx-Cache::> vserver peer create -vserver CacheSVM -peer-vserver OriginSVM -peer-
cluster Origin_ID -local-name OriginLocalName -application flexcache
```

2. No cluster de origem, use o comando a seguir para aceitar a relação de emparelhamento do SVM.

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-
name CacheLocalName
```

3. No cluster de origem, aceite a relação de emparelhamento.

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-
name CacheLocalName
```

4. Verifique se o emparelhamento do SVM foi bem-sucedido usando o seguinte comando; `Peer State` deve ser definido como `peered` na resposta.

```
Origin::> vserver peer show

Vserver      Peer Vserver    Peer State    Peering Cluster    Remote Applications

------------ --------------- ------------- ------------------
 ------------------------
OriginSVM    CacheSVM        peered        FSx-Cache          flexcache
```

Crie o FlexCache volume

Depois de criar com sucesso a relação de emparelhamento da SVM, a próxima etapa é criar o FlexCache volume na SVM do cache. O FlexCache volume deve ser umFlexGroup. Você também escolherá um modo de operação para seu FlexCache volume. Para obter mais informações, consulte FlexCachemodos de gravação.

1. No cluster de cache, use o seguinte comando ONTAP CLI para criar FlexCache seu volume. O exemplo cria um FlexCache volume de 2 TB chamado*CacheVol*.

   - Para criar um FlexCache volume de gravação, use o comando a seguir.

   ```
   FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
    -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
   aggr-list aggr1
   ```

   - Para criar um FlexCache volume de gravação, use o comando a seguir.

   ```
   FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
    -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
   aggr-list aggr1 -is-writeback-enabled true
   ```

   > **Note**
   >
   > Você pode usar o `volume flexcache config modify -is-writeback-enabled {true|false}`comando para modificar o modo de gravação. Antes de usar esse comando, certifique-se de entrar no modo avançado do ONTAP CLI usando o `set -privilege advanced`comando.

2. Verifique a FlexCache relação entre o FlexCache volume e o volume de origem.

   - Para um volume FlexCache de gravação, sua saída será semelhante ao exemplo a seguir.

   ```
   FSx-Cache::> volume flexcache show

   Vserver   Volume      Size     Origin-Vserver  Origin-Volume  Origin-Cluster
   -------   ----------  -------  --------------  -------------  --------------
   CacheSVM  CacheVol    2TB      OriginSVM       OriginVol      Origin
   ```

   - Para um volume FlexCache de gravação, sua saída será semelhante ao exemplo a seguir.

```
FSx-Cache::> volume flexcache show

Vserver   Volume      Size     Origin-Vserver  Origin-Volume  Origin-Cluster
 Writeback
-------   ----------  -------  --------------  -------------  --------------
 ---------
CacheSVM  CacheVol    2TB      OriginSVM       OriginVol      Origin
 true
```

Monte o FlexCache volume

Quando o FlexCache volume estiver DISPONÍVEL NFSv3 NFSv4, os clientes SMB poderão montá-lo. Depois de FlexCache montado, os clientes têm acesso a todo o conjunto de dados no volume de origem local.

- Para criar um ponto de montagem e montar o FlexCache, execute os seguintes comandos no cliente:

```
$ sudo mkdir -p /fsx/CacheVol
$ sudo mount -t nfs management.fs-01d2f606463087f6d.fsx.us-east-1.amazonaws.com:/
CacheVol /fsx/CacheVol
```

Replicando seus dados usando NetApp SnapMirror

Você pode usar: NetApp SnapMirror para agendar a replicação periódica do seu sistema de arquivos FSx for ONTAP de ou para um segundo sistema de arquivos. Esse recurso está disponível para implantações na região e entre regiões.

NetApp SnapMirror replica dados em alta velocidade, para que você obtenha alta disponibilidade de dados e rápida replicação de dados em todo ONTAP sistemas, se você estiver replicando entre dois sistemas de FSx arquivos da Amazon em AWS, ou do local para o. AWS A replicação pode ser programada a cada 5 minutos, embora os intervalos devam ser cuidadosamente escolhidos com base em RPOs (objetivos de ponto de recuperação), RTOs (objetivos de tempo de recuperação) e considerações de desempenho.

Quando você replica dados para NetApp sistemas de armazenamento e atualize continuamente os dados secundários, seus dados são mantidos atualizados e permanecem disponíveis sempre que

você precisar. Não são necessários servidores de replicação externos. Para obter mais informações sobre o uso NetApp SnapMirror para replicar seus dados, consulte Saiba mais sobre o serviço de replicação no NetApp BlueXP documentação.

Você pode criar um volume de destino de proteção de dados (DP) para NetApp SnapMirror usando o FSx console da Amazon AWS CLI, o e a FSx API da Amazon, além do NetApp ONTAP CLI e API REST. Para obter informações sobre a criação de um volume de destino usando o FSx console da Amazon AWS CLI, consulteComo criar volumes.

Você pode usar: NetApp BlueXP ou o ONTAP CLI para programar a replicação para seu sistema de arquivos.

> **Note**
>
> Existem dois tipos de SnapMirror replicação: em nível de volume SnapMirror e SVM Disaster Recovery (SVMDR). Somente em nível de volume SnapMirror a replicação é suportada pelo FSx for ONTAP. Synchronous SnapMirror, incluindo StrictSync, não é suportado.

O uso do NetApp BlueXP para programar a replicação

Você pode usar o NetApp BlueXP para configurar a replicação SnapMirror em seu sistema de arquivos FSx para ONTAP. Para obter mais informações, consulte Replicação de dados entre sistemas na documentação do NetApp BlueXP.

Usar o ONTAP CLI para programar a replicação

Você pode usar o ONTAP CLI para configurar a replicação de volume programada. Para obter informações, consulte Gerenciando a replicação de SnapMirror volumes no NetApp ONTAP Centro de documentação.

AWS relatórios de faturamento e uso FSx para ONTAP

AWS fornece dois relatórios de uso FSx para o ONTAP:

- O relatório AWS de cobrança é uma visão de alto nível de todas as atividades Serviços da AWS que você está usando, inclusive FSx do ONTAP.
- O relatório de AWS uso é um resumo da atividade de um serviço específico, agregado por hora, dia ou mês. Também inclui gráficos de uso que fornecem uma representação gráfica do seu uso FSx para o ONTAP.

> **Note**
>
> Como outros Serviços da AWS, FSx o ONTAP cobra apenas pelo que você usa. Para obter mais informações, consulte Amazon FSx for NetApp ONTAP Pricing.

Veja o relatório AWS de cobrança do FSx ONTAP

Você pode ver um resumo de seu AWS uso e cobranças, listados por serviço, na página Faturas no Gerenciamento de Faturamento e Custos da AWS console.

Para ver o relatório AWS de cobrança

1. Faça login no AWS Management Console e abra o Gerenciamento de Faturamento e Custos da AWS console em https://console.aws.amazon.com/costmanagement/.
2. No painel de navegação, escolha Faturas.
3. Escolha um período de cobrança (por exemplo, agosto de 2024).
4. Para ver FSx as cobranças da Amazon, na guia Cobranças por serviço, insira o campo de texto filtrar por serviço e, FSxem seguida, expanda FSxpara visualizar as cobranças por Região da AWS.

   As cobranças FSx pelos sistemas de arquivos ONTAP aparecem nas entradas Amazon:ONTAP FSx CreateFileSystem no relatório.
5. Para baixar o relatório de cobrança detalhado no formato CSV, escolha Baixar tudo para CSV na parte superior da página Faturas.

Para obter mais informações sobre sua AWS fatura, consulte Visualizar sua fatura no Guia do AWS Billing usuário.

O relatório de cobrança inclui os seguintes tipos de uso que se aplicam aos sistemas FSx de arquivos ONTAP:

First generation FSx for ONTAP file systems

Tipo de despesa	Unidades	Descrição
Armazenamento SSD ONTAP Single-AZ	GB por mês	A quantidade de armazenamento SSD provisionado em um sistema de arquivos ONTAP Single-AZ de primeira geração
Armazenamento SSD ONTAP Multi-AZ	GB por mês	A quantidade de armazenamento SSD provisionado em um sistema de arquivos FSx Multi-AZ para ONTAP de primeira geração
Capacidade de taxa de transferência ONTAP Single-AZ	MBps-Mês	A quantidade de capacidade de taxa de transferência provisionada em um sistema de arquivos FSx Single-AZ for ONTAP de primeira geração
Capacidade de taxa de transferência ONTAP Multi-AZ	MBps-Mês	A quantidade de capacidade de taxa de transferência provisionada em um sistema de arquivos FSx Multi-AZ para ONTAP de primeira geração
IOPS SSD ONTAP Single-AZ provisionado	Mês de IOPS	A quantidade de IOPS SSD provisionadas em um sistema de arquivos Single-

Tipo de despesa	Unidades	Descrição
		AZ para ONTAP de primeira geração FSx
IOPS SSD ONTAP Multi-AZ provisionado	Mês de IOPS	A quantidade de IOPS SSD provisionadas em um sistema de arquivos Multi-AZ para ONTAP de primeira geração FSx

Second generation FSx for ONTAP file systems

Tipo de despesa	Unidades	Descrição
Armazenamento SSD ONTAP Single-AZ-2	GB por mês	A quantidade de armazenamento SSD provisionado em um sistema de arquivos FSx Single-AZ para ONTAP de segunda geração
Armazenamento SSD ONTAP Multi-AZ-2	GB por mês	A quantidade de armazenamento SSD provisionado em um sistema de arquivos FSx Multi-AZ para ONTAP de segunda geração
Capacidade de taxa de transferência ONTAP Single-AZ-2	MBps-Mês	A quantidade de capacidade de taxa de transferência provisionada em um sistema de arquivos FSx Single-AZ for ONTAP de segunda geração
Capacidade de taxa de transferência ONTAP Multi-AZ-2	MBps-Mês	A quantidade de capacidade de taxa de transferência provisionada em um sistema

Tipo de despesa	Unidades	Descrição
		de arquivos FSx Multi-AZ para ONTAP de segunda geração
IOPS SSD ONTAP Single-AZ -2 provisionado	Mês de IOPS	A quantidade de IOPS SSD provisionadas em um sistema de arquivos Single-AZ para ONTAP de segunda geração FSx
IOPS SSD ONTAP Multi-AZ-2 provisionado	Mês de IOPS	A quantidade de IOPS SSD provisionadas em um sistema de arquivos Multi-AZ para ONTAP de segunda geração FSx

All FSx for ONTAP filesystems

Tipo de despesa	Unidades	Descrição
Armazenamento em pool de capacidade padrão ONTAP	GB por mês	A quantidade de armazenamento do pool de capacidade usada pelo sistema de arquivos FSx for ONTAP.
Armazenamento de backup ONTAP	GB por mês	A quantidade de capacidade de armazenamento usada para backups
SnapLock uso	GB por mês	A quantidade de capacidade de armazenamento usada pelo SnapLock volumes
	Operações	O número de solicitações de leitura feitas para o

Tipo de despesa	Unidades	Descrição	
Solicitações de leitura para o armazenamento de pool de capacidade padrão do ONTAP		armazenamento do pool de capacidade padrão em um sistema de arquivos FSx for ONTAP	
Grave solicitações para o armazenamento de pool de capacidade padrão do ONTAP	Operações	O número de solicitaç ões de gravação feitas no armazenamento do pool de capacidade padrão em um sistema de arquivos FSx for ONTAP	

Exibir o relatório AWS de uso FSx do ONTAP

AWS fornece um relatório FSx de uso mais detalhado do que o relatório de cobrança. O relatório de uso fornece dados de uso agregados por hora, dia ou mês e lista as operações por região e tipo de uso.

Para ver o relatório AWS de uso

1. Faça login no AWS Management Console e abra o Gerenciamento de Faturamento e Custos da AWS console em https://console.aws.amazon.com/costmanagement/.
2. No painel de navegação, escolha Explorador de Custos.
3. Na seção Parâmetros do relatório, escolha o intervalo de datas e a granularidade do seu relatório.
4. Deixe a dimensão Agrupar por > definida como Serviço.
5. Em Filtros > Serviço, escolha FSx
6. Escolha o Tipo de uso. Consulte a tabela abaixo deste procedimento para obter uma lista dos tipos de FSx uso do ONTAP.
7. Faça qualquer seleção de filtro adicional para seu relatório.
8. Para baixar os detalhes do relatório em um arquivo, escolha Baixar como CSV.

A tabela a seguir lista os FSx tipos de uso do ONTAP que você pode usar para filtrar o relatório e visualizar os dados de uso dos sistemas de arquivos ONTAP. Para obter mais informações sobre como usar o Cost Explorer, consulte Analisando seus custos e uso AWS Cost Explorer no Guia AWS Cost Management do Usuário.

First generation FSx for ONTAP file systems

Tipo de uso	Unidades	Descrição
region- Armazenamento. SAZ_2N: SSD	GB por mês	A quantidade de armazenamento SSD provisionado em um sistema de arquivos Single-AZ FSx for ONTAP de primeira geração.
region-Storage.maz: SSD	GB por mês	A quantidade de armazenamento SSD provisionado em um sistema de arquivos Multi-AZ FSx para ONTAP de primeira geração.
region- Throughpu tCapacity .SAZ_2N	MiBps-Não	A quantidade de capacidade de taxa de transferência provisionada em um sistema de arquivos Single-AZ FSx for ONTAP de primeira geração.
region-. ThroughputCapacity MAZ	MiBps-Não	A quantidade de capacidade de taxa de transferência provisionada em um sistema de arquivos Multi-AZ FSx para ONTAP de primeira geração.
region- SSDIOPS provisionado. SAZ_2N	IOPS-MO	A quantidade de IOPS de SSD provisionada acima de 3 IOPS por GiB de armazenamento SSD em um sistema de arquivos Single-AZ para ONTAP de primeira geração. FSx

Tipo de uso	Unidades	Descrição
region- SSDIOPS.maz provisionado	IOPS-MO	A quantidade de IOPS de SSD provisionada acima de 3 IOPS por GiB de armazenamento SSD em um sistema de arquivos Multi-AZ para ONTAP de primeira geração. FSx

Second generation FSx for ONTAP file systems

Tipo de uso	Unidades	Descrição
region- Armazenamento. SAZ_2N2: SSD	GB por mês	A quantidade de armazenamento SSD provisionado em um sistema de arquivos Single-AZ FSx for ONTAP de segunda geração.
region-Armazenamento. MAZ2:SSD	GB por mês	A quantidade de armazenamento SSD provisionado em um sistema de arquivos Multi-AZ FSx para ONTAP de segunda geração.
region- ThroughputCapacity .SAZ_2N2	MiBps-Não	A quantidade de capacidade de taxa de transferência provisionada em um sistema de arquivos Single-AZ FSx for ONTAP de segunda geração.
region-ThroughputCapacity.MAZ2	MiBps-Não	A quantidade de capacidade de taxa de transferência provisionada em um sistema de arquivos Multi-AZ FSx para ONTAP de segunda geração.
region- SSDIOPS provisionado. SAZ_2N2	IOPS-MO	A quantidade de IOPS de SSD provisionada acima de 3 IOPS por

Tipo de uso	Unidades	Descrição
		GiB de armazenamento SSD em um sistema de arquivos Single-AZ para ONTAP de segunda geração. FSx
region- SSDIOPs provisionados. MAZ2	IOPS-MO	A quantidade de IOPS de SSD provisionada acima de 3 IOPS por GiB de armazenamento SSD em um sistema de arquivos Multi-AZ para ONTAP de segunda geração. FSx

All FSx for ONTAP file systems

Tipo de uso	Unidades	Descrição
region-Storage.SAZ_2N: Padrão CPool	GB-Mo	A quantidade de armazenamento em pool de capacidade padrão usada em um sistema de arquivos Single-AZ FSx for ONTAP de primeira ou segunda geração.
region-Storage.maz: Padrão CPool	GB-Mo	A quantidade de armazenamento em pool de capacidade padrão usada em um sistema de arquivos Multi-AZ FSx para ONTAP de primeira ou segunda geração.
region-BackupUsage	GB por mês	A quantidade de capacidade de armazenamento usada para backups.
region-SnaplockUsage	GB por mês	A quantidade de capacidade de armazenamento usada pelo SnapLock volumes.

Tipo de uso	Unidades	Descrição
region-Solicitações. SAZ_2N: CPool StdRd	Operações	O número de solicitações de leitura feitas para o armazenamento de pool de capacidade padrão em um sistema de arquivos Single-AZ FSx for ONTAP.
region-Solicitações. SAZ_2N: CPool StdWr	Operações	O número de solicitações de gravação feitas no armazenamento de pool de capacidade padrão em um sistema de arquivos Single-AZ FSx for ONTAP.
region-Solicitações. MAZ: CPool StdRd	Operações	O número de solicitações de leitura feitas para o armazenamento de pool de capacidade padrão em um sistema de arquivos Multi-AZ FSx para ONTAP.
region-Solicitações. MAZ: CPool StdWr	Operações	O número de solicitações de gravação feitas no armazenamento de pool de capacidade padrão em um sistema de arquivos Multi-AZ FSx para ONTAP.

Monitorando a Amazon FSx para NetApp ONTAP

Você pode usar os seguintes serviços e ferramentas para monitorar o uso e a atividade do NetApp ONTAP na Amazon FSx :

- Amazon CloudWatch — Você pode monitorar sistemas de arquivos usando a Amazon CloudWatch, que coleta e processa automaticamente dados brutos do FSx ONTAP em métricas legíveis. Essas estatísticas são retidas por um período de 15 meses para que seja possível acessar informações históricas e ver a performance do sistema de arquivos. Você também pode definir alarmes com base nas suas métricas ao longo de um período especificado e realizar uma ou mais ações com base no valor das métricas em relação aos limites definidos por você.
- Eventos do ONTAP EMS — Você pode monitorar seu sistema FSx de arquivos do ONTAP usando eventos gerados pelo Sistema de Gerenciamento de Eventos (EMS) do ONTAP. Os eventos do EMS são notificações de ocorrências no sistema de arquivos, como a criação de LUN de iSCSI ou o dimensionamento automático de volumes.
- NetApp Informações sobre infraestrutura de dados — Você pode monitorar as métricas de configuração, capacidade e desempenho de seus sistemas de arquivos FSx para ONTAP usando o serviço NetApp Data Infrastructure Insights. Você também pode criar alertas com base nas condições das métricas.
- NetApp Harvest e NetApp Grafana — Você pode monitorar seu FSx sistema de arquivos ONTAP usando o Harvest NetApp e o Grafana. NetApp NetApp O Harvest monitora os sistemas de arquivos ONTAP coletando métricas de desempenho, capacidade e hardware dos sistemas FSx de arquivos ONTAP. O Grafana fornece um painel em que as métricas coletadas do Harvest podem ser exibidas.
- AWS CloudTrail— Você pode usar AWS CloudTrail para capturar todas as chamadas de API para a Amazon FSx como eventos. Esses eventos fornecem um registro das ações realizadas por um usuário, função ou AWS serviço na Amazon FSx.

Tópicos

- Monitoramento com a Amazon CloudWatch
- Monitoramento FSx de eventos do ONTAP EMS
- Monitoramento com insights de infraestrutura de dados
- Monitoramento FSx de sistemas de arquivos ONTAP usando Harvest e Grafana
- Monitoramento FSx de chamadas da API ONTAP com AWS CloudTrail

Monitoramento com a Amazon CloudWatch

Você pode monitorar sistemas de arquivos usando a Amazon CloudWatch, que coleta e processa dados brutos da Amazon FSx para NetApp ONTAP em métricas legíveis e quase em tempo real. Essas estatísticas são mantidas por um período de 15 meses, para que você possa acessar informações históricas para determinar o desempenho do seu sistema de arquivos. FSx para ONTAP, os dados métricos são enviados automaticamente CloudWatch em períodos de 1 minuto por padrão. Para obter mais informações sobre CloudWatch, consulte O que é a Amazon CloudWatch? no Guia do CloudWatch usuário da Amazon.

> **Note**
>
> Por padrão, o FSx for ONTAP envia dados métricos para CloudWatch períodos de 1 minuto, exceto as seguintes métricas que são enviadas em intervalos de 5 minutos:
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch as FSx métricas do ONTAP são organizadas em quatro categorias, que são definidas pelas dimensões usadas para consultar cada métrica. Para obter mais informações sobre dimensões, consulte Dimensões no Guia do CloudWatch usuário da Amazon.

- Métricas do sistema de arquivos: métricas de File-system-level desempenho e capacidade de armazenamento.
- Métricas do servidor de arquivos: File-server-level métricas.
- Métricas agregadas detalhadas do sistema de arquivos: métricas detalhadas do sistema de arquivos por agregado.
- Métricas detalhadas do sistema de arquivos: métricas File-system-level de armazenamento por nível de armazenamento (SSD e pool de capacidade).
- Métricas de volume: métricas de performance e capacidade de armazenamento por volume.
- Métricas detalhadas de volume: métricas de capacidade do armazenamento por volume pelo nível de armazenamento ou pelo tipo de dados (usuário, snapshot ou outro).

Todas as CloudWatch métricas do ONTAP são publicadas no `AWS/FSx` namespace em. FSx CloudWatch

Tópicos

- Acessando CloudWatch métricas
- Monitoramento no FSx console da Amazon
- Métricas do sistema de arquivos
- Métricas para sistemas de arquivos de segunda geração
- Métricas de volume

Acessando CloudWatch métricas

Você pode ver CloudWatch as métricas da Amazon FSx para a Amazon das seguintes formas:

- O FSx console da Amazon
- O CloudWatch console da Amazon
- O AWS Command Line Interface (AWS CLI) para CloudWatch
- A CloudWatch API

O procedimento a seguir explica como visualizar as CloudWatch métricas do seu sistema de arquivos com o FSx console da Amazon.

Para visualizar CloudWatch métricas do seu sistema de arquivos usando o FSx console da Amazon

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Sistemas de arquivos e selecione o sistema de arquivos cujas métricas você deseja visualizar.
3. Na página Resumo, escolha Monitoramento e performance no segundo painel para visualizar gráficos das métricas do sistema de arquivos.

Há quatro guias no painel Monitoramento e performance.

- Escolha Resumo (a guia padrão) para exibir quaisquer avisos, CloudWatch alarmes e gráficos ativos da atividade do sistema de arquivos.
- Escolha Armazenamento para visualizar a capacidade de armazenamento e as métricas de utilização.
- Escolha Performance para visualizar as métricas de performance do servidor de arquivos e do armazenamento.

- Escolha CloudWatch alarmes para ver gráficos de todos os alarmes configurados para seu sistema de arquivos.

O procedimento a seguir explica como visualizar as CloudWatch métricas do seu volume com o FSx console da Amazon.

Para visualizar CloudWatch as métricas do seu volume usando o FSx console da Amazon

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Volumes e selecione o volume cujas métricas você deseja visualizar.
3. Na página Resumo, escolha Monitoramento (a guia padrão) no segundo painel para visualizar gráficos com as métricas do volume.

O procedimento a seguir explica como visualizar as CloudWatch métricas do seu sistema de arquivos com o CloudWatch console da Amazon.

Para visualizar métricas usando o CloudWatch console da Amazon

1. Na página Resumo do sistema de arquivos, escolha Monitoramento e performance no segundo painel para visualizar gráficos das métricas do sistema de arquivos.
2. Escolha Visualizar em métricas no menu de ações no canto superior direito do gráfico que você deseja visualizar no CloudWatch console da Amazon. Isso abre a página Métricas no CloudWatch console da Amazon.

O procedimento a seguir explica como adicionar métricas do sistema FSx de arquivos ONTAP a um painel no CloudWatch console da Amazon.

Para adicionar métricas a um CloudWatch console da Amazon

1. Escolha o conjunto de métricas (resumo, armazenamento ou desempenho) no painel Monitoramento e desempenho do FSx console da Amazon.
2. Escolha Adicionar ao painel no canto superior direito do painel. Isso abre o CloudWatch console da Amazon.

3. Selecione um CloudWatch painel existente na lista ou crie um novo painel. Para obter mais informações, consulte Usando CloudWatch painéis da Amazon no Guia do CloudWatch usuário da Amazon.

O procedimento a seguir explica como acessar as métricas do sistema de arquivos com a AWS CLI.

Para acessar as métricas do AWS CLI

- Use o comando da CloudWatch CLI list-metrics com o parâmetro. `--namespace "AWS/FSx"` Para obter mais informações, consulte Referência de comandos da AWS CLI.

O procedimento a seguir explica como acessar as métricas do seu sistema de arquivos com a CloudWatch API.

Para acessar métricas da CloudWatch API

- Chame a operação da API GetMetricStatistics. Para obter mais informações, consulte a Amazon CloudWatch API Reference.

Monitoramento no FSx console da Amazon

As CloudWatch métricas relatadas pela Amazon FSx fornecem informações valiosas sobre seus sistemas FSx de arquivos e volumes do ONTAP.

Tópicos

- Monitoramento de métricas do sistema de arquivos no FSx console da Amazon
- Monitoramento de métricas de volume no FSx console da Amazon
- Avisos e recomendações de performance
- Criação de CloudWatch alarmes da Amazon para monitorar a Amazon FSx

Monitoramento de métricas do sistema de arquivos no FSx console da Amazon

Você pode usar o painel Monitoramento e desempenho no painel do seu sistema de arquivos no FSx console da Amazon para visualizar as métricas descritas na tabela a seguir. Para obter mais informações, consulte Acessando CloudWatch métricas.

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
Resumo	...determinar a quantidade da capacidade de armazenamento disponível no meu sistema de arquivos?	Capacidade de armazenamento principal disponível (bytes)	`StorageCapacity {SSD} - StorageUsed {SSD}`
	...determinar o throughput total do cliente do meu sistema de arquivos?	Throughput total do cliente (bytes por segundo)	SOMA(`DataReadBytes + DataWriteBytes`)/ PERÍODO (em segundos)
	...determinar o total de IOPS do cliente do meu sistema de arquivos?	Total de IOPS do cliente (operações por segundo)	SOMA(`DataReadOperations + DataWriteOperations + MetadataOperations`)/PERÍODO (em segundos)
	...determinar a latência média das operações de leitura, gravação e metadados do meu sistema de arquivos?	Latência média (ms/operação)	Latência média de leitura: `DataReadOperationTime * 1.000/DataReadOperations` Latência média de gravação: `DataWriteOperationTime * 1.000/DataWriteOperations`

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
			Latência média de metadados: `MetadataOperationTime * 1.000/MetadataOperations`
	...determinar a distribuição da capacidade de armazenamento usada e livre no meu sistema de arquivos?	Distribuição de armazenamento	Nível principal disponível: `StorageCapacity {SSD} - StorageUsed {SSD}` Nível principal usado: `StorageUsed {SSD}` Grupo de capacidade usado: `StorageUsed {StandardCapacityPool }`
	...determinar a economia com a eficiência do armazenamento (compressão, eliminação de duplicação e compactação)?	Economia com a eficiência do armazenamento	`StorageEfficiencySavings`
Armazenamento	...determinar a quantidade de armazenamento principal disponível?	Capacidade de armazenamento principal disponível (bytes)	`StorageCapacity {SSD} - StorageUsed {SSD}`

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
Performance do servidor de arquivos	...determinar a porcentagem de armazenamento principal usado do meu sistema de arquivos?	Utilização da capacidade de armazenamento principal (porcentagem)	`StorageUsed {SSD} * 100/StorageCapacity {SSD}`
	...determinar se meu sistema de arquivos está se aproximando do limite de throughput da rede?	Throughput da rede: utilização (porcentagem)	`NetworkThroughputUtilization`
	...determinar se meu sistema de arquivos está se aproximando do limite de throughput do disco?	Throughput do disco: utilização (porcentagem)	`FileServerDiskThroughputUtilization`
	...determinar se meu sistema de arquivos esgotou os créditos de intermitência permitidos para o throughput do disco?	Throughput de disco: equilíbrio de intermitência (porcentagem)	`FileServerDiskThroughputBalance`

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
	...determinar se meu sistema de arquivos está se aproximando do limite de IOPS de SSD dos servidores de arquivos?	IOPS de disco: utilização (porcentagem)	`FileServerDiskIopsUtilization`
	...determinar se meu sistema de arquivos esgotou os créditos de intermitência permitidos pelos servidores de arquivos para a IOPS de SSD de disco?	IOPS de disco: equilíbrio de intermitência (porcentagem)	`FileServerDiskIopsBalance`
	...determinar a utilização média da CPU do sistema de arquivos?	Utilização da CPU (porcentagem)	`CPUUtilization`
	... determinar se minha carga de trabalho está fazendo uso eficiente da RAM e dos caches de NVMe leitura do meu sistema de arquivos?	Proporção de ocorrência do cache (porcentagem)	`FileServerCacheHitRatio`

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
Performance do disco	...determinar se meu sistema de arquivos está se aproximando da capacidade de IOPS de SSD provisionada atualmente?	IOPS de disco: utilização (SSD) (porcentagem)	`DiskIopsUtilization`

> **Note**
>
> Recomendamos que você mantenha uma utilização média da capacidade de throughput de qualquer dimensão relacionada à performance, como utilização da rede, da CPU e da IOPS de SSD, abaixo de 50%. Isso garante que você tenha capacidade de throughput disponível suficiente para picos inesperados na sua workload, bem como para qualquer operação de armazenamento em segundo plano (como sincronização de armazenamento, divisão de dados em níveis ou backups).

Monitoramento de métricas de volume no FSx console da Amazon

Você pode ver o painel de monitoramento no painel do seu volume no FSx console da Amazon para ver métricas adicionais de desempenho. Para obter mais informações, consulte Acessando CloudWatch métricas.

Monitoramento	Como faço para...	Gráfico	Métricas relevantes
	...determinar a capacidade de armazenamento disponível do meu volume?	Capacidade de armazenamento	`StorageCapacity`

Monitoramento	Como faço para...	Gráfico	Métricas relevantes
		disponível	
	...determinar o throughput total de clientes do meu volume?	Throughput total do cliente (bytes por segundo)	SOMA(`DataReadBytes + DataWriteBytes`)/ PERÍODO (em segundos)
	...determinar o total de IOPS do cliente do meu volume?	Total de IOPS do cliente (operações por segundo)	SOMA(`DataReadOperations + DataWriteOperations + MetadataOperations`)/PERÍODO (em segundos)
	...determinar quantas operações de leitura e gravação estão vindo do nível do grupo de capacidade ou indo para ele?	IOPS do grupo de capacidade (operações por segundo)	Operações de leitura: `CapacityPoolReadOperations` Operações de gravação: `CapacityPoolWriteOperations`

Monitoramento	Como faço para...	Gráfico	Métricas relevantes
	...determinar a latência média das operações de leitura, gravação e metadados do meu volume?	Latência média (ms/operação)	Latência média de leitura: `DataReadOperationTime * 1.000/DataReadOperations` Latência média de gravação: `DataWriteOperationTime * 1.000/DataWriteOperations` Latência média de metadados: `MetadataOperationTime * 1.000/MetadataOperations`
	...determinar a quantidade de arquivos ou inodes disponíveis no meu volume?	Arquivos disponíveis (inodes)	`FilesCapacity - FilesUsed`
	...determinar a distribuição da capacidade de armazenamento usada e livre no meu volume?	Distribuição de armazenamento	`StorageCapacity - StorageUsed`

Avisos e recomendações de performance

FSx for ONTAP exibe um aviso para CloudWatch métricas sempre que uma dessas métricas se aproxima ou ultrapassa um limite predeterminado para vários pontos de dados consecutivos. Esses avisos fornecem recomendações práticas que você pode usar para otimizar a performance do seu sistema de arquivos.

Os avisos podem ser acessados em várias áreas do painel Monitoramento e performance. Todos os avisos de FSx desempenho ativos ou recentes da Amazon e todos CloudWatch os alarmes configurados para o sistema de arquivos que estão em um estado de ALARME aparecem no painel Monitoramento e desempenho na seção Resumo. O aviso também aparece na seção do painel onde o gráfico de métricas é exibido.

Você pode criar CloudWatch alarmes para qualquer uma das FSx métricas da Amazon. Para obter mais informações, consulte Criação de CloudWatch alarmes da Amazon para monitorar a Amazon FSx.

Use os avisos de performance para melhorar a performance do sistema de arquivos

FSx A Amazon fornece recomendações práticas que você pode usar para otimizar o desempenho do seu sistema de arquivos. Essas recomendações descrevem como lidar com um possível gargalo na performance. Você pode realizar a ação recomendada caso espere que a atividade continue ou se ela estiver causando um impacto na performance do seu sistema de arquivos. Dependendo da métrica que acionou um aviso, você pode resolvê-lo aumentando a capacidade de throughput ou a capacidade de armazenamento do sistema de arquivos, conforme descrito na tabela a seguir.

Seção do painel	Se houver um aviso para essa métrica	Faça o seguinte
Armazenamento	Utilização da capacidade de armazenamento principal	Aumente a capacidade de armazenamento principal do seu sistema de arquivos se ele ainda não estiver na capacidade máxima de armazenamento SSD. Para obter mais informações, consulte Atualizar a capacidade de armazenamento e as IOPS provisionadas. Se seu sistema de arquivos tiver vários pares de HA e sua utilização da capacidade de armazenamento principal for maior apenas para um subconjunto dos agregados do sistema de arquivos (os grupos de armazenamento que compõem seu nível de armazenamento principal), você também poderá reequilibrar sua workload para que a utilização da capacidade de armazenamento principal seja distribuída de maneira mais uniforme no sistema de arquivos. Para obter mais informações sobre o rebalanceamento

Seção do painel	Se houver um aviso para essa métrica	Faça o seguinte
		de workloads, consulte Equilibrando cargas de trabalho entre pares de HA.
Performance do servidor de arquivos	Throughput na rede	Aumente a capacidade de throughput do seu sistema de arquivos se ele ainda não estiver na capacidade máxima de throughput. Para mais informações sobre como atualizar a capacidade de throughput, consulte Atualizar a capacidade de throughput. Se o seu sistema de arquivos tiver vários pares de HA e a utilização for alta somente em um subconjunto de servidores de arquivos, você também poderá reequilibrar sua workload para que ela utilize de maneira mais uniforme os recursos de desempenho de cada um dos pares de HA do sistema de arquivos. Para obter mais informações sobre o rebalanceamento de workloads, consulte Equilibrando cargas de trabalho entre pares de HA.
	Throughput do disco	
	IOPS de disco	
	Utilização da CPU	

Seção do painel	Se houver um aviso para essa métrica	Faça o seguinte
Performance do disco	IOPS de disco	Aumente a IOPS de SSD se seu sistema de arquivos ainda não estiver no máximo de IOPS de SSD para a capacidade de throughput atual do seu sistema de arquivos. Para obter mais informações sobre como atualizar as IOPS provisionadas do seu sistema de arquivos, consulte Atualizar a capacidade de armazenamento e as IOPS provisionadas. Se seu sistema de arquivos tiver vários pares de HA e sua utilização da IOPS de disco for maior apenas para um subconjunto dos agregados do sistema de arquivos (os grupos de armazenamento que compõem seu nível de armazenamento principal), você também poderá reequilibrar sua workload para que suas IOPS de disco sejam utilizadas de maneira mais uniforme no sistema de arquivos. Para obter mais informaçõ es sobre o rebalanceamento de workloads, consulte Equilibrando cargas de trabalho entre pares de HA.

Para obter mais informações sobre a performance do sistema de arquivos, consulte Amazon FSx para desempenho do NetApp ONTAP.

Criação de CloudWatch alarmes da Amazon para monitorar a Amazon FSx

Você pode criar um CloudWatch alarme que envia uma mensagem do Amazon Simple Notification Service (Amazon SNS) quando o alarme muda de estado. Um alarme observa uma única métrica por um período tempo que você especifica. Se necessário, o alarme realiza uma ou mais ações com base no valor da métrica relativa a um determinado limite durante vários períodos. A ação é uma notificação enviada a um tópico do Amazon SNS ou a uma política de Auto Scaling.

Os alarmes invocam ações somente para mudanças de estado sustentadas. CloudWatch os alarmes não invocam ações somente porque estão em um estado específico; o estado deve ter sido alterado e mantido por um determinado número de períodos. Você pode criar um alarme no FSx console da Amazon ou no CloudWatch console da Amazon.

Os procedimentos a seguir descrevem como criar alarmes usando o FSx console, AWS Command Line Interface (AWS CLI) e a API da Amazon.

Para definir alarmes usando o console da Amazon FSx

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Sistemas de arquivos e selecione o sistema de arquivos para o qual deseja criar o alarme.
3. Na página Resumo, escolha Monitoramento e performance no segundo painel.
4. Escolha a guia CloudWatch de alarmes.
5. Escolha Criar CloudWatch alarme. O sistema redireciona você para o console do CloudWatch.
6. Escolha Selecionar métrica.
7. Na seção Métricas, escolha FSx.
8. Escolha uma categoria de métrica:
   - Métricas do sistema de arquivos
   - Métricas detalhadas do sistema de arquivos
   - Métricas de volume
   - Métricas detalhadas de volume
9. Escolha a métrica para a qual você deseja definir o alarme e Selecionar métrica.
10. Na seção Condições, escolha as condições desejadas para o alarme e selecione Próximo.

    > **Note**
    >
    > As métricas podem não ser publicadas durante a manutenção do sistema de arquivos. Para evitar alterações desnecessárias e enganosas nas condições de alarme e configurar seus alarmes para que sejam resilientes aos pontos de dados perdidos, consulte Como configurar como os CloudWatch alarmes tratam os dados perdidos no Guia do usuário da Amazon. CloudWatch

11. Se você quiser CloudWatch enviar um e-mail ou uma notificação ao Amazon SNS quando o estado do alarme iniciar a ação, escolha um estado de alarme para o gatilho do estado do alarme.

    Em Enviar uma notificação ao seguinte tópico do SNS, escolha uma opção. Se escolher Create topic (Criar tópico), você poderá definir o nome e o endereço de e-mail para uma nova lista de

assinaturas de e-mail. Essa lista é salva e aparece no campo para alarmes futuros. Escolha Próximo.

> **Note**
>
> Se você usar Create topic (Criar tópico) para criar um novo tópico do Amazon SNS, os endereços de e-mail deverão ser verificados antes que eles recebam notificações. Os e-mails são enviados somente quando o alerta entra em um estado de alerta. Se essa alteração no status de alarme ocorrer antes que os endereços de e-mail sejam verificados, eles não receberão notificação.

12. Preencha os campos Nome do alarme e Descrição do alarme e selecione Próximo.
13. Na página Pré-visualizar e criar, revise o alarme que está prestes a criar e escolha Criar alarme.

Para definir alarmes usando o console CloudWatch

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Escolha Criar alarme para iniciar o Assistente de criação de alarmes.
3. Siga o procedimento em Para definir alarmes usando o FSx console da Amazon, começando com a etapa 6.

Para definir um alarme usando o AWS CLI

- Chame o put-metric-alarmcomando CLI. Para obter mais informações, consulte Referência de comandos da AWS CLI.

Para definir um alarme usando a CloudWatch API

- Chame a operação da API PutMetricAlarm. Para obter mais informações, consulte a Amazon CloudWatch API Reference.

Métricas do sistema de arquivos

As métricas do sistema de arquivos Amazon FSx for NetApp ONTAP são classificadas como métricas do sistema de arquivos ou métricas detalhadas do sistema de arquivos.

- As Métricas do sistema de arquivos são métricas agregadas de performance e armazenamento para um único sistema de arquivos que assume uma única dimensão, `FileSystemId`. Essas métricas medem a performance da rede e o uso da capacidade de armazenamento do seu sistema de arquivos.
- As Métricas detalhadas do sistema de arquivos medem a capacidade de armazenamento do sistema de arquivos e o armazenamento usado em cada nível de armazenamento (por exemplo, armazenamento SSD e armazenamento em grupo de capacidade). Cada métrica inclui uma dimensão `FileSystemId`, `StorageTier` e `DataType`.

Observe o seguinte sobre quando a Amazon FSx publica pontos de dados para essas métricas para CloudWatch:

- Para as métricas de utilização (qualquer métrica cujo nome termine em Utilization, como`NetworkThroughputUtilization`), há um ponto de dados emitido a cada período para cada servidor de arquivos ativo ou agregado. Por exemplo, a Amazon FSx emite uma métrica minuciosa por servidor de arquivos ativo e uma métrica minuciosa por agregado para`FileServerDiskIopsUtilization`. `DiskIopsUtilization`
- Para todas as outras métricas, há um único ponto de dados emitido a cada período, correspondendo ao valor total da métrica em todos os seus servidores de arquivos ativos (como `DataReadBytes` para métricas de servidores de arquivos) ou em todos os seus agregados (como `DiskReadBytes` para métricas de armazenamento).

Tópicos

- Métricas de E/S de rede
- Métricas do servidor de arquivos
- Métricas de E/S de disco
- Métricas da capacidade de armazenamento
- Métricas detalhadas do sistema de arquivos

Métricas de E/S de rede

Todas essas métricas assumem uma dimensão, `FileSystemId`.

Métrica	Descrição
`NetworkThroughputUtilization`	O percentual de utilização do throughput de rede do sistema de arquivos. A estatística `Average` é a utilização média do throughput da rede do sistema de arquivos em um período especificado. A estatística `Minimum` é a menor utilização do throughput da rede do sistema de arquivos em um período especificado. A estatística `Maximum` é a maior utilização do throughput da rede do sistema de arquivos em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`NetworkSentBytes`	O número de bytes (E/S de rede) enviados pelo sistema de arquivos. A estatística `Sum` é o número total de bytes enviados pelo sistema de arquivos em um período especificado. Para calcular o throughput enviado (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período especific ado. Unidades: bytes Estatísticas válidas: `Sum`
`NetworkReceivedBytes`	O número de bytes (E/S de rede) recebidos pelo sistema de arquivos.

Métrica	Descrição
	A estatística `Sum` é o número total de bytes recebidos pelo sistema de arquivos em um período especificado. Para calcular o throughput recebido (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período especific ado. Unidades: bytes Estatísticas válidas: `Sum`
`DataReadBytes`	O número de bytes (E/S de rede) das leituras feitas por clientes no sistema de arquivos. A estatística `Sum` é o número total de bytes associados às operações de leitura no período especificado. Para calcular a média de throughput (bytes por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: bytes Estatísticas válidas: `Sum`

Métrica	Descrição
`DataWriteBytes`	O número de bytes (E/S de rede) das gravações feitas por clientes no sistema de arquivos. A estatística `Sum` é o número total de bytes associados às operações de gravação no período especificado. Para calcular a média de throughput (bytes por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: bytes Estatísticas válidas: `Sum`
`DataReadOperations`	A contagem das operações de leitura (E/S de rede) das leituras feitas por clientes no sistema de arquivos. A estatística `Sum` é o número total de operações de E/S que ocorreram em um período especificado. Para calcular a média de operações de leitura por segundo para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatísticas válidas: `Sum`

Métrica	Descrição
`DataWriteOperations`	A contagem das operações de gravação (E/S de rede) das gravações feitas por clientes no sistema de arquivos. A estatística `Sum` é o número total de operações de E/S que ocorreram em um período especificado. Para calcular a média de operações de gravação por segundo para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatísticas válidas: `Sum`
`MetadataOperations`	A contagem das operações de metadados (E/S de rede) feitas por clientes no sistema de arquivos. A estatística `Sum` é o número total de operações de E/S que ocorreram em um período especificado. Para calcular a média de operações de metadados por segundo para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatísticas válidas: `Sum`

Métrica	Descrição
`DataReadOperationTime`	A soma do tempo total gasto no sistema de arquivos em operações de leitura (E/S de rede) feitas por clientes acessando dados no sistema de arquivos. A estatística `Sum` é o número total de segundos gastos pelas operações de leitura no período especificado. Para calcular a latência média de leitura de um período, divida a estatística `Sum` pela `Sum` da métrica `DataReadOperations` no mesmo período. Unidades: segundos Estatísticas válidas: `Sum`
`DataWriteOperationTime`	A soma do tempo total gasto no sistema de arquivos para realizar operações de gravação (E/S de rede) feitas por clientes acessando dados no sistema de arquivos. A estatística `Sum` é o número total de segundos gastos pelas operações de gravação durante o período especificado. Para calcular a latência média de gravação em um período, divida a estatística `Sum` pela `Sum` da métrica `DataWriteOperations` no mesmo período. Unidades: segundos Estatísticas válidas: `Sum`

Métrica	Descrição
`CapacityPoolReadBytes`	O número de bytes lidos (E/S de rede) do nível do grupo de capacidade do sistema de arquivos. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de bytes lidos do nível do grupo de capacidade do sistema de arquivos em um período especific ado. Para calcular os bytes do grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especific ado. Unidades: bytes Estatísticas válidas: `Sum`

Métrica	Descrição
`CapacityPoolReadOperations`	O número de operações de leitura (E/S de rede) do nível do grupo de capacidade do sistema de arquivos. Isso se traduz em uma solicitação de leitura do grupo de capacidade. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de operações de leitura do nível do grupo de capacidade do sistema de arquivos em um período especificado. Para calcular as solicitações de grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especificado. Unidades: contagem Estatísticas válidas: `Sum`

Métrica	Descrição
`CapacityPoolWriteBytes`	O número de bytes gravados (E/S de rede) no nível do grupo de capacidade do sistema de arquivos. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de bytes gravados no nível do grupo de capacidad e do sistema de arquivos em um período especificado. Para calcular os bytes do grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especific ado. Unidades: bytes Estatísticas válidas: `Sum`

Métrica	Descrição
`CapacityPoolWriteOperations`	O número de operações de gravação (E/S de rede) no sistema de arquivos do nível do grupo de capacidade. Isso se traduz em uma solicitação de gravação. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de operações de gravação no nível do grupo de capacidade do sistema de arquivos em um período especificado. Para calcular as solicitações de grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especificado. Unidades: contagem Estatísticas válidas: `Sum`

Métricas do servidor de arquivos

Todas essas métricas assumem uma dimensão, `FileSystemId`.

Métrica	Descrição
`CPUUtilization`	A porcentagem de utilização dos recursos de CPU do sistema de arquivos. A estatística `Average` é a utilização média da CPU do sistema de arquivos em um período especificado.

Métrica	Descrição
	A estatística `Minimum` é a menor utilização da CPU do sistema de arquivos em um período especificado. A estatística `Maximum` é a maior utilização da CPU do sistema de arquivos em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`FileServerDiskThroughputUtilization`	O throughput do disco entre o servidor de arquivos e a camada principal, como uma porcentagem do limite provisionado determinado pela capacidade de throughput. A estatística `Average` é a porcentagem média de utilização do throughput de disco dos servidores de arquivos em um período especificado. A estatística `Minimum` é a menor porcentagem de utilização do throughput de disco dos servidores de arquivos em um período especificado. A estatística `Maximum` é a maior utilização do throughput de disco dos servidores de arquivos em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerDiskThroughputBalance`	A porcentagem de créditos de intermitência disponíveis para throughput de disco entre o servidor de arquivos e o nível principal. Isso é válido para sistemas de arquivos provisionados com uma capacidade de taxa de transferência inferior a 512. MBps A estatística `Average` é o equilíbrio médio de intermitência disponível em um período especificado. A estatística `Minimum` é o equilíbrio mínimo de intermitência disponível em um período especificado. A estatística `Maximum` é o equilíbrio máximo de intermitência disponível em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerDiskIopsBalance`	A porcentagem de créditos de intermitência disponíveis para IOPS de disco entre o servidor de arquivos e o nível principal. Isso é válido para sistemas de arquivos provisionados com uma capacidade de taxa de transferência inferior a 512. MBps A estatística `Average` é o equilíbrio médio de intermitência disponível em um período especificado. A estatística `Minimum` é o equilíbrio mínimo de intermitência disponível em um período especificado. A estatística `Maximum` é o equilíbrio máximo de intermitência disponível em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerDiskIopsUtilization`	A porcentagem de utilização de IOPS da capacidade de IOPS de disco disponível para o servidor de arquivos. A estatística `Average` é a utilização média de IOPS de disco do sistema de arquivos em um período especificado. A estatística `Minimum` é a utilização mínima de IOPS de disco do sistema de arquivos em um período especificado. A estatística `Maximum` é a utilização máxima de IOPS de disco do sistema de arquivos em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerCacheHitRatio`	A porcentagem de todas as solicitações de leitura atendidas pelos dados na RAM e nos NVMe caches do sistema de arquivos. Uma porcentagem maior significa que mais leituras são atendidas pelos caches de leitura do sistema de arquivos. Unidades: percentual A estatística `Average` é a porcentagem média de ocorrência do cache do sistema de arquivos em um período especificado. A estatística `Minimum` é a menor porcentagem de ocorrência do cache do sistema de arquivos em um período especificado. A estatística `Maximum` é a maior porcentagem de ocorrência do cache do sistema de arquivos em um período especificado. Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métricas de E/S de disco

Todas essas métricas assumem uma dimensão, `FileSystemId`.

Métrica	Descrição
`DiskReadBytes`	O número de bytes (E/S de disco) de qualquer leitura de disco na camada principal do sistema de arquivos.

Métrica	Descrição
	A estatística `Sum` é o número total de bytes lidos do sistema de arquivos em um período especificado. Para calcular o throughput de leitura do disco (bytes por segundo) para qualquer estatísti ca, divida a estatística `Sum` pelos segundos no período especificado. Unidades: bytes Estatísticas válidas: `Sum`
`DiskWriteBytes`	O número de bytes (E/S de disco) de qualquer gravação do disco no nível principal do sistema de arquivos. A estatística `Sum` é o número total de bytes gravados do sistema de arquivos em um período especificado. Para calcular o throughput de gravação do disco (bytes por segundo) para qualquer estatística, divida a estatística `Sum` pelos segundos no período especificado. Unidades: bytes Estatísticas válidas: `Sum`

Métrica	Descrição
`DiskIopsUtilization`	A IOPS de disco entre o servidor de arquivos e os volumes de armazenamento, como uma porcentagem do limite de IOPS do disco provisionado nos níveis principais. A estatística `Average` é a utilização média de IOPS de disco do sistema de arquivos em um período especificado. A estatística `Minimum` é a utilização mínima de IOPS de disco do sistema de arquivos em um período especificado. A estatística `Maximum` é a utilização máxima de IOPS de disco do sistema de arquivos em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`DiskReadOperations`	O número de operações de leitura (E/S de disco) da camada principal do sistema de arquivos. A estatística `Sum` é o número total de operações de leitura da camada principal em um período especificado. Unidades: contagem Estatísticas válidas: `Sum`

Métrica	Descrição
`DiskWriteOperations`	O número de operações de gravação (E/S de disco) no nível principal do sistema de arquivos. A estatística `Sum` é o número total de operações de gravação na camada principal em um período especificado. Unidades: contagem Estatísticas válidas: `Sum`

Métricas da capacidade de armazenamento

Todas essas métricas assumem uma dimensão, `FileSystemId`.

Métrica	Descrição
`StorageEfficiencySavings`	Os bytes economizados com os recursos de eficiência do armazenamento (compressão, eliminação de duplicação e compactação). A estatística `Average` é a economia média com a eficiência de armazenamento em um período especificado. Para calcular a economia com a eficiência do armazenamento como uma porcentagem de todos os dados armazenados, em um período de um minuto, divida `StorageEfficiencySavings` pela soma de `StorageEfficiencySavings` e pela métrica `StorageUsed` do sistema de arquivos, usando a estatística `Sum` para `StorageUsed` .

Métrica	Descrição
	A estatística `Minimum` é a economia mínima com a eficiência do armazenamento em um período especificado. A estatística `Maximum` é a economia máxima com a eficiência do armazenamento em um período especificado. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`StorageUsed`	A quantidade total de dados físicos armazenados no sistema de arquivos, tanto no nível principal (SSD) quanto no nível do grupo de capacidade. Essa métrica inclui economias com recursos de eficiência do armazenamento, como compressão e eliminação de duplicação dos dados. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`LogicalDataStored`	A quantidade total de dados lógicos armazenados no sistema de arquivos, considerando tanto o nível SSD quanto o nível do grupo de capacidade. Essa métrica inclui o tamanho lógico total dos instantâneos e FlexClones, mas não inclui a economia de eficiência de armazenamento obtida por meio da compactação, compactação e desduplicação. Para computar a economia com a eficiência do armazenamento em bytes, pegue a `Average` de `StorageUsed` em um determinado período e subtraia da `Average` de `LogicalDataStored` no mesmo período. Para computar a economia com a eficiência do armazenamento como uma porcentagem do tamanho lógico total dos dados, pegue a `Average` de `StorageUsed` em um determinado período e subtraia da `Average` de `LogicalDataStored` no mesmo período. Em seguida, divida a diferença pela `Average` de `LogicalDataStored` no mesmo período. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métricas detalhadas do sistema de arquivos

As métricas detalhadas do sistema de arquivos são métricas detalhadas de utilização do armazenamento para cada um dos seus níveis de armazenamento. Todas as métricas detalhadas do sistema de arquivos têm as dimensões `FileSystemId`, `StorageTier` e `DataType`.

- A dimensão `StorageTier` indica o nível de armazenamento medido pela métrica, com valores possíveis de `SSD` e `StandardCapacityPool`.
- A dimensão `DataType` indica o tipo de dados medidos pela métrica, com o valor possível de `All`.

Há uma linha para cada combinação exclusiva de um determinado par de chave-valor métrico e dimensional, com uma descrição do que essa combinação mede.

Métrica	Descrição
`StorageCapacityUtilization`	A utilização da capacidade de armazenamento para cada um dos agregados do seu sistema de arquivos. Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A estatística `Average` é a quantidade média de utilização da capacidade de armazenamento para o nível de desempenho do seu sistema de arquivos durante o período especificado. A estatística `Minimum` é a menor quantidad e de utilização da capacidade de armazenam ento para o nível de desempenho do seu sistema de arquivos durante o período especificado. A estatística `Maximum` é a maior quantidade de utilização da capacidade de armazenamento para o nível de desempenho do seu sistema de arquivos durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`StorageCapacity`	A capacidade total de armazenamento do nível principal (SSD).

Métrica	Descrição
	Unidades: bytes Estatísticas válidas: `Maximum`

Métrica	Descrição
`StorageUsed`	A capacidade de armazenamento físico usada em bytes, específica do nível de armazenam ento. Esse valor inclui economias com recursos de eficiência do armazenamento, como compressão e eliminação de duplicação dos dados. Os valores de dimensão válidos para `StorageTier` são `SSD` e `StandardC apacityPool` , correspondendo ao nível de armazenamento medido por essa métrica. Essa métrica também exige a dimensão `DataType` com o valor de `All`. As estatísticas `Average`, `Minimum` e `Maximum` são o consumo de armazenamento por nível em bytes para o período determinado. Para calcular a utilização da capacidade de armazenamento do nível de armazenamento principal (SSD), divida qualquer uma dessas estatísticas pelo `Maximum` da `StorageCa pacity` no mesmo período, com a dimensão `StorageTier` igual ao `SSD`. Para calcular a capacidade de armazenam ento livre do nível de armazenamento principal (SSD) em bytes, subtraia qualquer uma dessas estatísticas do `Maximum` da `StorageCa pacity` no mesmo período, com a dimensão `StorageTier` igual ao `SSD`. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métricas para sistemas de arquivos de segunda geração

As métricas a seguir são fornecidas FSx para os sistemas de arquivos de segunda geração do ONTAP. Para as métricas, um ponto de dados é emitido para cada par de HA e para cada agregado (para métricas de utilização de armazenamento).

> **Note**
>
> Se você tiver um sistema de arquivos com vários pares de HA, também poderá usar as métricas do sistema de arquivos com um único par de HA e as métricas de volume.

Tópicos

- Métricas de E/S de rede
- Métricas do servidor de arquivos
- Métricas de E/S de disco
- Métricas detalhadas do sistema de arquivos

Métricas de E/S de rede

Todas essas métricas assumem duas dimensões, `FileSystemId` e `FileServer`.

- `FileSystemId`— ID do AWS recurso do seu sistema de arquivos.
- `FileServer`: o nome de um servidor de arquivos (ou nó) no ONTAP (por exemplo, `FsxId01234567890abcdef-01`). Os servidores de arquivos com números ímpares são servidores preferenciais de arquivos (ou seja, eles atendem ao tráfego, a menos que o sistema de arquivos tenha feito failover para o servidor de arquivos secundário), enquanto os servidores de arquivos com números pares são servidores secundários de arquivos (ou seja, eles só atendem ao tráfego quando o par não estiver disponível). Por esse motivo, os servidores secundários de arquivos costumam mostrar menos utilização do que os servidores preferenciais de arquivos.

Métrica	Descrição
`NetworkThroughputUtilization`	Utilização do throughput de rede como uma porcentagem do throughput de rede disponíve l para seu sistema de arquivos. Essa métrica é

Métrica	Descrição
	equivalente ao máximo `NetworkSentBytes` e `NetworkReceivedBytes` como uma porcentagem da capacidade de throughput de rede de um par de HA para seu sistema de arquivos. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado dos servidores de arquivos do seu sistema de arquivos. A estatística `Average` é a utilização média do throughput da rede para o respectivo servidor de arquivos durante o período especificado. A estatística `Minimum` é a menor utilização do throughput da rede para o respectivo servidor de arquivos no decorrer de um minuto durante o período especificado. A estatística `Maximum` é a maior utilização do throughput da rede para o respectivo servidor de arquivos no decorrer de um minuto durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`NetworkSentBytes`	O número de bytes (E/S de rede) enviados por seu sistema de arquivos. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado dos servidores de arquivos do seu sistema de arquivos. A estatística `Sum` é o número total de bytes enviados pela rede usando o respectivo servidor de arquivos durante o período especificado. A estatística `Average` é o número médio de bytes enviados pela rede usando o respectivo servidor de arquivos durante o período especificado. A estatística `Minimum` é o menor número de bytes enviados pela rede usando o respectivo servidor de arquivos durante o período especificado. A estatística `Maximum` é o maior número de bytes enviados pela rede usando o respectivo servidor de arquivos durante o período especificado. Para calcular o throughput enviado (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período especificado. Unidades: bytes

Métrica	Descrição
	Estatísticas válidas: `Sum`, `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`NetworkReceivedBytes`	O número de bytes (E/S de rede) recebidos por seu sistema de arquivos. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado dos servidores de arquivos do seu sistema de arquivos. A estatística `Sum` é o número total de bytes recebidos pela rede usando o respectivo servidor de arquivos durante o período especificado. A estatística `Average` é o número médio de bytes recebidos pela rede usando o respectivo servidor de arquivos a cada minuto durante o período especificado. A estatística `Minimum` é o menor número de bytes recebidos pela rede usando o respectivo servidor de arquivos a cada minuto durante o período especificado. A estatística `Maximum` é o maior número de bytes recebidos pela rede usando o respectivo servidor de arquivos a cada minuto durante o período especificado. Para calcular o throughput recebido (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período. Unidades: bytes Estatísticas válidas: `Sum`, `Average`, `Minimum` e `Maximum`

Métricas do servidor de arquivos

Todas essas métricas assumem duas dimensões, `FileSystemId` e `FileServer`.

Métrica	Descrição
`CPUUtilization`	A porcentagem de utilização dos recursos de CPU do sistema de arquivos. Há uma métrica emitida a cada minuto para cada agregado dos servidores de arquivos do seu sistema de arquivos. A estatística `Average` é a utilização média da CPU do sistema de arquivos em um período especificado. A estatística `Minimum` é a menor utilização da CPU para o respectivo servidor de arquivos durante o período especificado. A estatística `Maximum` é a maior utilização da CPU para o respectivo servidor de arquivos durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`FileServerDiskThroughputUtilization`	O throughput do disco entre o servidor de arquivos e o agregado, como uma porcentagem do limite provisionado determinado pela capacidade de throughput. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Essa métrica é equivalente à soma de `DiskReadBytes` e `DiskWriteBytes` como uma porcentagem da capacidade de throughput de disco do servidor de

Métrica	Descrição
	arquivos de um par de HA para seu sistema de arquivos. Há uma métrica emitida a cada minuto para cada agregado dos servidores de arquivos do seu sistema de arquivos. A estatística `Average` é a utilização média do throughput de disco do servidor de arquivos para o respectivo servidor de arquivos durante o período especificado. A estatística `Minimum` é a menor utilização do throughput de disco do servidor de arquivos para o respectivo servidor de arquivos durante o período especificado. A estatística `Maximum` é a maior utilização do throughput de disco do servidor de arquivos para o respectivo servidor de arquivos durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerDiskIopsUtilization`	A utilização de IOPS da capacidade de IOPS de disco disponível para seu servidor de arquivos, como uma porcentagem do limite de IOPS de disco. Isso é diferente de `DiskIopsUtilization` por ser a utilização de IOPS de disco em relação ao máximo atendido por seu servidor de arquivos, ao contrário da sua IOPS de disco provisionada. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado dos servidores de arquivos do seu sistema de arquivos. A estatística `Average` é a utilização média da IOPS de disco do servidor de arquivos durante o período especificado. A estatística `Minimum` é a menor utilização da IOPS de disco do servidor de arquivos para o respectivo servidor de arquivos durante o período especificado. A estatística `Maximum` é a maior utilização da IOPS de disco do servidor de arquivos para o respectivo servidor de arquivos durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerCacheHitRatio`	A porcentagem de todas as solicitações de leitura atendidas pelos dados que residem na RAM ou nos NVMe caches do sistema de arquivos para cada um dos pares de HA (por exemplo, o servidor de arquivos ativo em um par de HA). Uma porcentagem maior indica uma proporção maior de leituras em cache em relação ao total de leituras. Toda a I/O é considerada, inclusive tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado dos servidores de arquivos do seu sistema de arquivos. Unidades: percentual A estatística `Average` é a proporção média de ocorrências do cache para um dos pares de HA do seu sistema de arquivos durante um período especificado. A estatística `Minimum` é a menor proporção de ocorrências do cache para um dos pares de HA do seu sistema de arquivos durante um período especificado. A estatística `Maximum` é a maior proporção de ocorrências do cache para um dos pares de HA do seu sistema de arquivos durante um período especificado. Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métricas de E/S de disco

Todas essas métricas assumem duas dimensões, `FileSystemId` e `Aggregate`.

- `FileSystemId`— ID do AWS recurso do seu sistema de arquivos.
- `Aggregate`: o nível de desempenho do seu sistema de arquivos consiste em vários grupos de armazenamento chamados de agregados. Há um agregado para cada par de HA. Por exemplo, o agregado `aggr1` está mapeado para o servidor de arquivos `FsxId01234567890abcdef-01` (o servidor de arquivos ativo) e o servidor de arquivos `FsxId01234567890abcdef-02` (o servidor de arquivos secundário) em um par de HA.

Métrica	Descrição
`DiskReadBytes`	O número de bytes (E/S do disco) de qualquer leitura de disco desse agregado. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirro r hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A estatística `Sum` é o número total de bytes lidos a cada minuto do respectivo agregado durante o período especificado. A estatística `Average` é o número médio de bytes lidos a cada minuto do respectivo agregado durante o período especificado. A estatística `Minimum` é o menor número de bytes lidos a cada minuto do respectivo agregado durante o período especificado. A estatística `Maximum` é o maior número de bytes lidos a cada minuto do respectivo agregado durante o período especificado.

Métrica	Descrição
	Para calcular o throughput de leitura de disco (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período. Unidades: bytes Estatísticas válidas: `Sum`, `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`DiskWriteBytes`	O número de bytes (E/S do disco) de qualquer gravação de disco desse agregado. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirro r hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A estatística `Sum` é o número total de bytes gravados no respectivo agregado durante o período especificado. A estatística `Average` é o número médio de bytes gravados no respectivo agregado a cada minuto durante o período especificado. A estatística `Minimum` é o menor número de bytes gravados no respectivo agregado a cada minuto durante o período especificado. A estatística `Maximum` é o maior número de bytes gravados no respectivo agregado a cada minuto durante o período especificado. Para calcular o throughput de gravação do disco (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período especificado. Unidades: bytes Estatísticas válidas: `Sum`, `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`DiskIopsUtilization`	A utilização de IOPS em disco de um agregado, como uma porcentagem do limite de IOPS de disco do agregado (ou seja, o total de IOPS do sistema de arquivos dividido pelo número de pares de HA para seu sistema de arquivos). Isso difere de `FileServe rDiskIopsUtilization` por ser a utilização de IOPS de disco provisionado em relação ao limite de IOPS provisionadas, ao contrário do máximo de IOPS de disco suportado pelo servidor de arquivos (ou seja, determinado pela capacidade de throughput configurada por par de HA). Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarqui zação e backups). Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A estatística `Average` é a utilização média da IOPS de disco do respectivo agregado durante o período especificado. A estatística `Minimum` é a menor utilização da IOPS de disco do respectivo agregado durante o período especificado. A estatística `Maximum` é a maior utilização da IOPS de disco do respectivo agregado durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`DiskReadOperations`	O número de operações de leitura (E/S de disco) para esse agregado. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A estatística `Sum` é o número total de operações de leitura realizadas pelo respectivo agregado durante o período especificado. A estatística `Average` é o número médio de operações de leitura realizadas a cada minuto pelo respectivo agregado durante o período especificado. A estatística `Minimum` é o menor número de operações de leitura realizadas a cada minuto pelo respectivo agregado durante o período especificado. A estatística `Maximum` é o maior número de operações de leitura realizadas a cada minuto pelo respectivo agregado durante o período especificado. Para calcular a média de IOPS de disco durante o período, use a estatística `Average` e divida o resultado por 60 (segundos). Unidades: contagem Estatísticas válidas: `Sum`, `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`DiskWriteOperations`	O número de operações de gravação (E/S de disco) para esse agregado. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A estatística `Sum` é o número total de operações de gravação realizadas pelo respectivo agregado durante o período especificado. A estatística `Average` é o número médio de operações de gravação realizadas a cada minuto pelo respectivo agregado durante o período especificado. Para calcular a média de IOPS de disco durante o período, use a estatística `Average` e divida o resultado por 60 (segundos). Unidades: contagem Estatísticas válidas: `Sum` e `Average`

Métricas detalhadas do sistema de arquivos

As métricas detalhadas do sistema de arquivos são métricas detalhadas de utilização do armazenamento para cada um dos seus níveis de armazenamento. As métricas detalhadas do sistema de arquivos têm as dimensões `FileSystemId`, `StorageTier` e `DataType` ou as dimensões `FileSystemId`, `StorageTier`, `DataType` e `Aggregate`.

- Quando a dimensão `Aggregate` não é fornecida, as métricas servem para todo o seu sistema de arquivos. As métricas `StorageUsed` e `StorageCapacity` têm um único ponto de dados a cada minuto correspondente ao armazenamento total consumido do sistema de arquivos (por nível de

armazenamento) e à capacidade total de armazenamento (para o nível SSD). Enquanto isso, a métrica `StorageCapacityUtilization` emite uma métrica a cada minuto para cada agregado.

- Quando a dimensão `Aggregate` é fornecida, as métricas são para cada agregado.

O significado das dimensões é o seguinte:

- `FileSystemId`— ID do AWS recurso do seu sistema de arquivos.
- `Aggregate`: o nível de desempenho do seu sistema de arquivos consiste em vários grupos de armazenamento chamados de agregados. Há um agregado para cada par de HA. Por exemplo, o agregado `aggr1` está mapeado para o servidor de arquivos `FsxId01234567890abcdef-01` (o servidor de arquivos ativo) e o servidor de arquivos `FsxId01234567890abcdef-02` (o servidor de arquivos secundário) em um par de HA.
- `StorageTier`: indica o nível de armazenamento medido pela métrica, com os valores possíveis de `SSD` e `StandardCapacityPool`.
- `DataType`: indica o tipo de dados medido pela métrica, com o valor possível de `All`.

Há uma linha para cada combinação exclusiva de um determinado par de chave-valor métrico e dimensional, com uma descrição do que essa combinação mede.

Métrica	Descrição
`StorageCapacityUtilization`	A utilização da capacidade de armazenamento para um determinado agregado de sistema de arquivos. Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A estatística `Average` é a quantidade média de utilização da capacidade de armazenam ento para um determinado agregado durante o período especificado. A estatística `Minimum` é a quantidade mínima de utilização da capacidade de armazenam ento para um determinado agregado durante o período especificado.

Métrica	Descrição
	A estatística `Maximum` é a quantidade máxima de utilização da capacidade de armazenam ento para um determinado agregado durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`StorageCapacity`	A capacidade de armazenamento para um determinado agregado de sistema de arquivos. Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A estatística `Average` é a quantidade média de capacidade de armazenamento para um determinado agregado durante o período especificado. A estatística `Minimum` é a quantidade mínima de capacidade de armazenamento para um determinado agregado durante o período especificado. A estatística `Maximum` é a quantidade máxima de capacidade de armazenamento para um determinado agregado durante o período especificado. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`StorageUsed`	A capacidade de armazenamento físico usada em bytes, específica do nível de armazenam ento. Esse valor inclui economias com recursos de eficiência do armazenamento, como compressão e eliminação de duplicação dos dados. Os valores de dimensão válidos para `StorageTier` são `SSD` e `StandardC apacityPool` , correspondendo ao nível de armazenamento medido por essa métrica. Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A estatística `Average` é a quantidade média de capacidade de armazenamento físico consumida no respectivo nível de armazenam ento pelo agregado especificado durante o período especificado. A estatística `Minimum` é a quantidade mínima de capacidade de armazenamento físico consumida no respectivo nível de armazenam ento pelo agregado especificado durante o período especificado. A estatística `Maximum` é a quantidade máxima de capacidade de armazenamento físico consumida no respectivo nível de armazenam ento pelo agregado especificado durante o período especificado. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métricas de volume

Seu sistema de arquivos Amazon FSx for NetApp ONTAP pode ter um ou mais volumes que armazenam seus dados. Cada um desses volumes tem um conjunto de CloudWatch métricas, classificadas como métricas de volume ou métricas de volume detalhadas.

- As Métricas de volume são métricas de performance e armazenamento por volume que assumem duas dimensões: `FileSystemId` e `VolumeId`. `FileSystemId` mapeia para o sistema de arquivos ao qual o volume pertence.
- Métricas de volume detalhadas são per-storage-tier métricas que medem o consumo de armazenamento por nível com a `StorageTier` dimensão (com valores possíveis de `SSD` e`StandardCapacityPool`) e por tipo de dados com a `DataType` dimensão (com valores possíveis de `UserSnapshot`, e`Other`). Essas métricas têm as dimensões `FileSystemId`, `VolumeId`, `StorageTier` e `DataType`.

Tópicos

- Métricas de E/S de rede
- Métricas da capacidade de armazenamento
- Métricas detalhadas de volume

Métricas de E/S de rede

Todas essas métricas assumem duas dimensões, `FileSystemId` e `VolumeId`.

Métrica	Descrição
`DataReadBytes`	O número de bytes (E/S de rede) lidos do volume pelos clientes. A estatística `Sum` é o número total de bytes associados às operações de leitura no período especificado. Para calcular a média de throughput (bytes por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: bytes

Métrica	Descrição
	Estatísticas válidas: `Sum`
`DataWriteBytes`	O número de bytes (E/S de rede) gravados no volume pelos clientes. A estatística `Sum` é o número total de bytes associados às operações de gravação no período especificado. Para calcular a média de throughput (bytes por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: bytes Estatísticas válidas: `Sum`
`DataReadOperations`	O número de operações de leitura (E/S de rede) no volume feitas por clientes. A estatística `Sum` é o número total das operações de leitura no período especificado. Para calcular a média de operações de leitura por segundo para um período, divida a estatísti ca `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatísticas válidas: `Sum`

Métrica	Descrição
`DataWriteOperations`	O número de operações de gravação (E/S de rede) no volume feitas por clientes. A estatística `Sum` é o número total das operações de gravação no período especific ado. Para calcular a média de operações de gravação por segundo para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatísticas válidas: `Sum`
`MetadataOperations`	O número de operações de E/S (E/S de rede) das atividades de metadados feitas por clientes no volume. A estatística `Sum` é o número total das operações de metadados no período especific ado. Para calcular a média de operações de metadados por segundo para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatísticas válidas: `Sum`

Métrica	Descrição
`DataReadOperationTime`	A soma do tempo total gasto no volume para operações de leitura (E/S de rede) de clientes acessando dados no volume. A estatística `Sum` é o número total de segundos gastos pelas operações de leitura no período especificado. Para calcular a latência média de leitura de um período, divida a estatística `Sum` pela `Sum` da métrica `DataReadOperations` no mesmo período. Unidades: segundos Estatísticas válidas: `Sum`
`DataWriteOperationTime`	A soma do tempo total gasto no volume para realizar operações de gravação (E/S de rede) de clientes acessando dados no volume. A estatística `Sum` é o número total de segundos gastos pelas operações de gravação durante o período especificado. Para calcular a latência média de gravação em um período, divida a estatística `Sum` pela `Sum` da métrica `DataWriteOperations` no mesmo período. Unidades: segundos Estatísticas válidas: `Sum`

Métrica	Descrição
`MetadataOperationTime`	A soma do tempo total gasto no volume para realizar operações de metadados (E/S de rede) de clientes acessando dados no volume. A estatística `Sum` é o número total de segundos gastos pelas operações de leitura no período especificado. Para calcular a latência média de um período, divida a estatística `Sum` pela `Sum` das `MetadataOperations` no mesmo período. Unidades: segundos Estatísticas válidas: `Sum`
`CapacityPoolReadBytes`	O número de bytes lidos (E/S de rede) do nível do grupo de capacidade do volume. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de bytes lidos do nível do grupo de capacidade do volume em um período especificado. Para calcular os bytes do grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especificado. Unidades: bytes Estatísticas válidas: `Sum`

Métrica	Descrição
`CapacityPoolReadOperations`	O número de operações de leitura (E/S de rede) do nível do grupo de capacidade do volume. Isso se traduz em uma solicitação de leitura do grupo de capacidade. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de operações de leitura do nível do grupo de capacidade do volume em um período especific ado. Para calcular as solicitações de grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especific ado. Unidades: contagem Estatísticas válidas: `Sum`

Métrica	Descrição
`CapacityPoolWriteBytes`	O número de bytes gravados (E/S de rede) no nível do grupo de capacidade do volume. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de bytes gravados no nível do grupo de capacidade do volume em um período especificado. Para calcular os bytes do grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especificado. Unidades: bytes Estatísticas válidas: `Sum`

Métrica	Descrição
`CapacityPoolWriteOperations`	O número de operações de gravação (E/S de rede) no volume do nível do grupo de capacidade. Isso se traduz em uma solicitação de gravação. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de operações de gravação no nível do grupo de capacidade do volume em um período especificado. Para calcular as solicitações de grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especificado. Unidades: contagem Estatísticas válidas: `Sum`

Métricas da capacidade de armazenamento

Todas essas métricas assumem duas dimensões, `FileSystemId` e `VolumeId`.

Métrica	Descrição
`StorageCapacity`	O tamanho do volume em bytes. Unidades: bytes Estatísticas válidas: `Maximum`
`StorageUsed`	A capacidade de armazenamento lógico usada do volume.

Métrica	Descrição
	Unidades: bytes Estatísticas válidas: `Average`
`StorageCapacityUtilization`	A utilização da capacidade de armazenamento do volume. Unidades: percentual Estatísticas válidas: `Average`
`FilesUsed`	Os arquivos usados (número de arquivos ou inodes) no volume. Unidades: contagem Estatísticas válidas: `Average`
`FilesCapacity`	O número total de inodes que podem ser criados no volume. Unidades: contagem Estatísticas válidas: `Maximum`

Métricas detalhadas de volume

As métricas detalhadas de volume assumem mais dimensões do que as métricas de volume, permitindo medições mais granulares dos seus dados. Todas as métricas detalhadas de volume têm as dimensões `FileSystemId`, `VolumeId`, `StorageTier` e `DataType`.

- A dimensão `StorageTier` indica o nível de armazenamento medido pela métrica, com valores possíveis de `All`, `SSD` e `StandardCapacityPool`.
- A dimensão `DataType` indica o tipo de dados medidos pela métrica, com valores possíveis de `All`, `User`, `Snapshot` e `Other`.

A tabela a seguir define o que é medido pela métrica `StorageUsed` para as dimensões listadas.

Métrica	Descrição
`StorageUsed`	A quantidade de espaço lógico usado, em bytes. Essa métrica mede diferentes tipos de consumo de espaço, dependendo das dimensões usadas com ela. Ao definir o `StorageTier` como `SSD` ou `StandardCapacityPool` e configurar o `DataType` como `All`, essa métrica mede o uso do espaço lógico desse volume para os níveis de SSD e grupo de capacidade, respectivamente. Ao definir a dimensão `DataType` como `User`, `Snapshot` ou `Other` e configurar o `StorageTier` como `All`, essa métrica mede o uso do espaço lógico para cada tipo respectivo de dados. O consumo de dados do `Snapshot` inclui a reserva de snapshot, que é 5% do tamanho do volume por padrão. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`StorageCapacityUtilization`	A porcentagem do espaço físico em disco usado pelo volume. Unidades: percentual Estatísticas válidas: `Maximum`

Monitoramento FSx de eventos do ONTAP EMS

Você pode monitorar os eventos do sistema FSx de arquivos ONTAP usando o Sistema de Gerenciamento de Eventos (EMS) nativo do NetApp ONTAP. Você pode visualizar esses eventos usando a CLI do NetApp ONTAP.

Tópicos

- Visão geral dos eventos EMS
- Visualização de eventos EMS
- Encaminhamento de eventos do EMS para um servidor Syslog

Visão geral dos eventos EMS

Os eventos do EMS são notificações geradas automaticamente que alertam você quando uma condição predefinida ocorre em seu sistema de arquivos FSx for ONTAP. Essas notificações mantêm você informado para que você possa evitar ou corrigir problemas que podem levar a problemas maiores, como aqueles de autenticação de máquina virtual de armazenamento (SVM) ou volumes cheios.

Por padrão, os eventos são registrados no log do sistema de gerenciamento de eventos. Usando o EMS, você pode monitorar eventos como alterações na senha do usuário, um componente com capacidade quase FlexGroup total, um número de unidade lógica (LUN) colocado manualmente on-line ou off-line ou um volume redimensionado automaticamente.

Para obter mais informações sobre eventos do ONTAP EMS, consulte Referência do ONTAP EMS no Centro de Documentação do NetApp ONTAP. Para exibir as categorias de eventos, use o painel de navegação esquerdo do documento.

> **Note**
>
> Somente algumas mensagens do ONTAP EMS estão disponíveis FSx para sistemas de arquivos ONTAP. Para ver uma lista das mensagens do ONTAP EMS disponíveis, use o comando show do catálogo de eventos do NetApp ONTAP CLI.

As descrições de eventos EMS contêm nomes de eventos, gravidade, possíveis causas, mensagens de log e ações corretivas que podem ajudar você a decidir como responder. Por exemplo, um evento wafl.vol.autosize.Fail ocorre quando o dimensionamento automático de um volume falha. De acordo com a descrição do evento, a ação corretiva é aumentar o tamanho máximo do volume ao definir o tamanho automático.

Visualização de eventos EMS

Use o comando NetApp ONTAP CLI event log show para exibir o conteúdo do registro de eventos. Esse comando estará disponível se você tiver o perfil `fsxadmin` em seu sistema de arquivos. A sintaxe do comando é a seguinte:

```
event log show [event_options]
```

Os eventos mais recentes são listados primeiro. Por padrão, esse comando exibe os eventos de nível de gravidade `EMERGENCY`, `ALERT` e `ERROR` com as seguintes informações:

- Hora: a hora do evento.
- Nó: o nó em que o evento ocorreu.
- Gravidade: o nível de gravidade do evento. Para exibir os eventos de nível de gravidade `NOTICE`, `INFORMATIONAL` ou `DEBUG`, use a opção `-severity`.
- Evento: o nome e a mensagem do evento.

Para exibir informações detalhadas sobre eventos, use uma ou mais das opções de eventos listadas na tabela a seguir.

Opção de evento	Descrição
`-detail`	Exibe informações adicionais sobre o evento.
`-detailtime`	Exibe informações detalhadas do evento em ordem cronológica inversa.
`-instance`	Exibe informações detalhadas sobre todos os campos.
`-node nodename|local`	Exibe uma lista de eventos para o nó que você especifica. Use essa opção com `-seqnum` para exibir informações detalhadas.

Opção de evento	Descrição
`-seqnum` *sequence_number*	Seleciona os eventos que correspondem a esse número na sequência. Use com `-node` para exibir informações detalhadas.

Opção de evento	Descrição

`-time MM/DD/YYYY HH:MM:SS`	Seleciona os eventos que aconteceram nesse horário específico. Use o formato: MM/DD/YYYY HH:MM:SS [+-HH:MM]. Você pode especificar um intervalo de tempo usando o operador `..` entre duas declarações de tempo.
	`event log show -time "04/17/2023 05:55:00".."04/17/2023 06:10:00"`
	Os valores comparativos de tempo são relativos à hora atual quando você executa o comando. O exemplo a seguir mostra como exibir apenas eventos que ocorreram no último minuto:
	`event log show -time >1m`
	Os campos de mês e data dessa opção não são preenchidos com zero. Esses campos podem ter dígito únicos; por exemplo, `4/1/2023 06:45:00`.

Opção de evento	Descrição
`-severity sev_level`	Seleciona os eventos que correspondem ao *sev_level* valor, que deve ser um dos seguintes: • `EMERGENCY` : interrupção • `ALERT`: único ponto de falha • `ERROR`: redução • `NOTICE`: informações • `INFORMATIONAL` : informações • `DEBUG`: informações de depuração Para exibir todos os eventos, especifique a gravidade da seguinte forma: `event log show -severity <=DEBUG`

Opção de evento	Descrição
`-ems-severity` *ems_sev_level*	Seleciona os eventos que correspondem ao *ems_sev_level* valor, que deve ser um dos seguintes: • `NODE_FAULT` : a corrupção de dados é detectada ou o nó não consegue fornecer atendimento ao cliente. • `SVC_FAULT` : uma perda temporária de serviço, normalmente uma falha transitória, é detectada. • `NODE_ERROR` : um erro de hardware que não é imediatamente fatal é detectado. • `SVC_ERROR` : um erro de software que não é imediatamente fatal é detectado. • `WARNING`: uma mensagem de alta prioridade que não indica uma falha. • `NOTICE`: uma mensagem de prioridade normal que não indica uma falha. • `INFO`: uma mensagem de baixa prioridade que não indica uma falha. • `DEBUG`: uma mensagem de depuração.

Opção de evento	Descrição
	• VAR: uma mensagem com gravidade variável, selecionada no runtime. Para exibir todos os eventos, especifique a gravidade da seguinte forma: `event log show -ems-severity <=DEBUG`
`-source` *`text`*	Seleciona os eventos que correspondem ao *`text`* valor. Normalmente, a fonte é um módulo de software.
`-message-name` *`message_name`*	Seleciona os eventos que correspondem ao *`message_name`* valor. Os nomes das mensagens são descritivos; portanto, a filtragem da saída por nome da mensagem exibe mensagens de um tipo específico.
`-event` *`text`*	Seleciona os eventos que correspondem ao *`text`* valor. O campo `event` contém o texto completo do evento, incluindo todos os parâmetros.

Opção de evento	Descrição
`-kernel-generation-num` *integer*	Seleciona os eventos que correspondem ao *integer* valor. Somente eventos provenientes do kernel têm números de geração do kernel.
`-kernel-sequence-num` *integer*	Seleciona os eventos que correspondem ao *integer* valor. Somente eventos provenientes do kernel têm números de sequência do kernel.
`-action` *text*	Seleciona os eventos que correspondem ao *text* valor. O campo `action` descreve qual ação corretiva , se houver, você deve tomar para remediar a situação.
`-description` *text*	Seleciona os eventos que correspondem ao *text* valor. O campo `description` descreve por que o evento aconteceu e o que isso significa.
`-filter-name` *filter_name*	Seleciona os eventos que correspondem ao *filter_name* valor. Somente os eventos incluídos pelos filtros existentes que correspondem a esse valor são exibidos.

Opção de evento	Descrição
`-fields` *`fieldname ,...`*	Indica que a saída do comando também inclui os campos especificados. Você pode usar `-fields ?` para escolher os campos que deseja especificar.

Visualizar eventos EMS

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar o NetApp ONTAP CLI do usuário do Amazon FSx for NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Use o comando `event log show` para exibir o conteúdo do log de eventos.

   ```
   ::> event log show
   Time                Node          Severity      Event
   ------------------- ------------- ------------- ------------------------
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0a.
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0d.
   ```

Para obter informações sobre os eventos do EMS retornados pelo `event log show` comando, consulte a Referência do ONTAP EMS no Centro de Documentação do NetApp ONTAP.

Encaminhamento de eventos do EMS para um servidor Syslog

Você pode configurar eventos do EMS para encaminhar notificações para um servidor Syslog. O encaminhamento de eventos do EMS é usado para monitorar em tempo real seu sistema de arquivos a fim de determinar e isolar as causas básicas de uma ampla variedade de problemas. Caso o ambiente ainda não tenha um servidor Syslog para notificações de eventos, será necessário criar um. O DNS deverá ser configurado no sistema de arquivos para resolver o nome do servidor Syslog.

> **Note**
>
> O destino do Syslog deve estar localizado na sub-rede primária usada pelo sistema de arquivos.

Para configurar eventos do EMS para encaminhar notificações para um servidor Syslog

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar o NetApp ONTAP CLI do usuário do Amazon FSx for NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Use o comando event notification destination create para criar um destino de notificação de eventos do tipo `syslog`, especificando os seguintes atributos:

   - *`dest_name`*: o nome do destino da notificação que deve ser criado (por exemplo, `syslog-ems`). O nome de um destino de notificação de evento deve ter de 2 a 64 caracteres. Os caracteres válidos são os seguintes caracteres ASCII: A-Z, a-z, 0-9, “_” e “-”. O nome deve começar e terminar com: A-Z, a-z ou 0-9.
   - *`syslog_name`*: o nome do host ou endereço IP do servidor Syslog para o qual as mensagens do Syslog são enviadas.
   - *`transport_protocol`*: o protocolo usado para enviar os eventos.
     - `udp-unencrypted`: protocolo de datagrama de usuário sem segurança. Esse é o protocolo padrão.
     - `tcp-unencrypted`: protocolo de controle de transmissão sem segurança.
     - `tcp-encrypted`: o protocolo de controle de transmissão com Transport Layer Security (TLS). Quando essa opção é especificada, o FSx for ONTAP verifica a identidade do host de destino validando seu certificado.
   - *`port_number`*: a porta do servidor Syslog para o qual as mensagens do Syslog são enviadas. O parâmetro `syslog-port` com valor padrão depende da configuração do parâmetro `syslog-transport`. Se `syslog-transport` estiver definido como `tcp-encrypted`, o valor padrão de `syslog-port` será `6514`. Se `syslog-transport` estiver definido como `tcp-unencrypted`, `syslog-port` terá o valor padrão de `601`. Caso contrário, a porta padrão será definida como `514`.

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. Use o comando event notification create para criar uma nova notificação de um conjunto de eventos definido por um filtro de eventos para o destino da notificação criado na etapa anterior, especificando os seguintes atributos:

   - *node_name*: o nome do filtro de evento. Os eventos incluídos no filtro de eventos são encaminhados para os destinos especificados no parâmetro `-destinations`.
   - *dest_name*: o nome do destino de notificação existente para o qual as notificações de eventos são enviadas.

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. Se tiver selecionado TCP como o *transport_protocol*, você pode usar o comando `event notification destination check` para gerar uma mensagem de teste e verificar se a configuração funciona. Especifique os seguintes atributos com o comando:

   - *node_name*: o nome do nó (por exemplo, `FsxId07353f551e6b557b4-01`).
   - *dest_name*: o nome do destino de notificação existente para o qual as notificações de eventos são enviadas.

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

Monitoramento com insights de infraestrutura de dados

NetApp O Data Infrastructure Insights (antigo Cloud Insights) é um NetApp serviço que você pode usar para monitorar seus sistemas de arquivos Amazon FSx for NetApp ONTAP junto com suas outras soluções NetApp de armazenamento. Com o Data Infrastructure Insights, você pode monitorar as métricas de configuração, capacidade e desempenho ao longo do tempo para entender as tendências de sua carga de trabalho e planejar as necessidades futuras de desempenho e capacidade de armazenamento. Você também pode criar alertas com base nas condições de

métricas que podem ser integradas aos seus fluxos de trabalho e ferramentas de produtividade existentes.

> **Note**
>
> O Data Infrastructure Insights não é compatível com sistemas de arquivos de segunda geração com mais de um par de HA.

O Data Infrastructure Insights fornece:

- Uma variedade de métricas e logs: colete métricas de configuração, capacidade e performance. Entenda a tendência da sua workload com painéis, alertas e relatórios predefinidos.
- Analytics de usuário e proteção contra ransomware: com os snapshots do Cloud Secure e do ONTAP, você pode auditar, detectar, interromper e reparar incidentes de erro do usuário e ransomware.
- SnapMirror relatórios — entenda seus SnapMirror relacionamentos e defina alertas sobre problemas de replicação.
- Planejamento de capacidade — entenda os requisitos de recursos das cargas de trabalho locais para ajudá-lo a migrar sua carga de trabalho para uma configuração mais eficiente FSx do ONTAP. Você também pode usar esses insights para planejar quando será necessário mais desempenho ou capacidade FSx para sua implantação no ONTAP.

Para obter mais informações, consulte a documentação do Data Infrastructure Insights na documentação do produto NetApp ONTAP.

Monitoramento FSx de sistemas de arquivos ONTAP usando Harvest e Grafana

NetApp O Harvest é uma ferramenta de código aberto para coletar métricas de desempenho e capacidade dos sistemas ONTAP e é compatível com FSx o ONTAP. Você pode usar o Harvest com Grafana para uma solução de monitoramento de código aberto.

Conceitos básicos do Harvest e Grafana

A seção a seguir detalha como você pode configurar o Harvest e o Grafana para medir o desempenho e a utilização FSx da capacidade de armazenamento do sistema de arquivos ONTAP.

Você pode monitorar seu sistema de arquivos Amazon FSx for NetApp ONTAP usando Harvest and Grafana. NetApp Harvest monitores ONTAP data centers coletando métricas de desempenho, capacidade e hardware dos sistemas FSx de arquivos ONTAP. Grafana fornece um painel onde os coletados Harvest métricas podem ser exibidas.

Painéis compatíveis do Harvest

O Amazon FSx for NetApp ONTAP expõe um conjunto de métricas diferente do que o local NetApp ONTAP. Portanto, somente o seguinte out-of-the-box Harvest Atualmente, os painéis marcados com `fsx` são compatíveis para uso com o FSx ONTAP. Alguns desses painéis podem não apresentar as informações que não são compatíveis.

- Colheita: Metadados
- ENDEREÇO: cDOT
- ONTAP: Cluster
- ONTAP: conformidade
- ONTAP: Centro de dados
- ONTAP: snapshots de proteção de dados
- BOTÃO: LUN
- ONTAP: Modo
- ENDEREÇO: Qtree
- ONTAP: segurança
- TOQUE EM: SnapMirror
- ONTAP: SVM
- ONTAP: volume

Os seguintes exemplos de Harvest os painéis são compatíveis com o FSx for ONTAP, mas não são habilitados por padrão no Harvest.

- TOQUE EM: FlexCache
- TOQUE EM: FlexGroup
- ONTAP: Clientes NFS
- ONTAP: Monitores NFSv4 Storepool
- ONTAP: Solução de problemas de NFS

- ENCAIXE: SMB
- ONTAP: Carga de trabalho

Sem compatibilidade Harvest painéis

Os seguintes exemplos de Harvest os painéis não são compatíveis com o FSx for ONTAP.

- ONTAP: Agregado
- ONTAP: Disco
- ONTAP: Operação de serviço externo
- ONTAP: Análise de sistemas de arquivos (FSA)
- ONTAP: Health
- TOQUE EM: MetroCluster
- ONTAP: Potência
- ONTAP: Prateleira
- ONTAP: Armazenamentos de objetos do S3

AWS CloudFormation modelo

Para começar, você pode implantar um AWS CloudFormation modelo que inicia automaticamente uma EC2 instância da Amazon executando Harvest e Grafana. Como entrada para o AWS CloudFormation modelo, você especifica o `fsxadmin` usuário e o endpoint FSx de gerenciamento da Amazon para o sistema de arquivos que será adicionado como parte dessa implantação. Depois que a implantação for concluída, você poderá fazer login no painel do Grafana para monitorar seu sistema de arquivos.

Essa solução é usada AWS CloudFormation para automatizar a implantação da solução Harvest e Grafana. O modelo cria uma instância Amazon EC2 Linux e instala os softwares Harvest e Grafana. Para usar essa solução, baixe o fsx-ontap-harvest-grafanamodelo AWS CloudFormation .template.

> **Note**
>
> A implementação dessa solução gera cobrança pelos serviços associados AWS . Para obter mais informações, consulte as páginas de detalhes de preços desses serviços.

Tipos de EC2 instância da Amazon

Ao configurar o modelo, você fornece o tipo de EC2 instância da Amazon. NetAppA recomendação da para o tamanho da instância depende de quantos sistemas de arquivos você monitora e do número de métricas que você escolhe coletar. Com a configuração padrão, para cada 10 sistemas de arquivos que você monitora, NetApp recomenda:

- CPU: dois núcleos
- Memória: 1 GB
- Disco: 500 MB (usado principalmente por arquivos de log)

Veja a seguir alguns exemplos de configurações e o tipo de instância `t3` que você pode escolher.

Sistemas de arquivos	CPU	Disk	Tipo de instância
Menos de 10	2 núcleos	500 MB	`t3.micro`
De 10 a 40	4 núcleos	1.000 MB	`t3.xlarge`
40+	8 núcleos	2.000 MB	`t3.2xlarge`

Para obter mais informações sobre os tipos de EC2 instância da Amazon, consulte Instâncias de uso geral no Guia EC2 do usuário da Amazon.

Regras de porta para instância

Ao configurar sua EC2 instância da Amazon, certifique-se de que as portas 3000 e 9090 estejam abertas para tráfego de entrada para o grupo de segurança em que as instâncias Amazon EC2 Harvest e Grafana estão. Como a instância iniciada se conecta a um endpoint por HTTPS, ela precisa resolver o endpoint, que precisa da porta 53 TCP/UDP para DNS. Além disso, para alcançar o endpoint, ele precisa da porta 443 TCP para HTTPS e acesso à Internet.

Procedimento de implantação

O procedimento a seguir configura e implanta a solução Harvest e Grafana. A implantação demora cerca de cinco minutos. Antes de começar, você deve ter um sistema de arquivos FSx for ONTAP em execução em uma Amazon Virtual Private Cloud (Amazon VPC) em AWS sua conta e as

informações de parâmetros para o modelo listado abaixo. Para obter mais informações sobre como criar um sistema de arquivos, consulte Criar sistemas de arquivos.

Executar a pilha de soluções Harvest e Grafana

1. Baixe o fsx-ontap-harvest-grafanamodelo AWS CloudFormation .template. Para obter mais informações sobre como criar uma AWS CloudFormation pilha, consulte Como criar uma pilha no AWS CloudFormation console no Guia do AWS CloudFormation usuário.

   > **Note**
   >
   > Por padrão, esse modelo é iniciado na AWS região Leste dos EUA (Norte da Virgínia). Você deve iniciar essa solução em um Região da AWS local onde a Amazon FSx esteja disponível. Para obter mais informações, consulte FSx endpoints e cotas da Amazon no.Referência geral da AWS

2. Em Parâmetros, analise os parâmetros para o modelo e modifique-os de acordo com as necessidades do seu sistema de arquivos. Essa solução usa os valores padrão apresentados a seguir.

Parameter	Padrão	Descrição
InstanceType	`t3.micro`	O tipo de EC2 instância da Amazon. A seguir, estão os tipos de instância `t3`. • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` Para ver a lista completa dos valores de tipo de EC2 instância da Amazon

Parameter	Padrão	Descrição
		permitidos para esse parâmetro, consulte o fsx-ontap-harvest-grafana arquivo.template.
KeyPair	Nenhum valor padrão	O par de chaves usado para acessar a EC2 instância da Amazon.
SecurityGroup	Nenhum valor padrão	O ID do grupo de segurança da instância do Harvest e Grafana. Certifique-se de que as portas de entrada 3000 e 9090 (além das portas 53 e 443) estejam abertas dos clientes que você deseja usar para acessar seu painel do Grafana.
Tipo de sub-rede	Nenhum valor padrão	Especifique o tipo de sub-rede, `public` ou `private`. Use uma sub-rede `public` para recursos que devem estar conectados à Internet e uma sub-rede privada para recursos que não estarão conectados à Internet. Para obter mais informações, consulte Tipos de sub-redes no Guia do usuário da Amazon VPC.

Parameter	Padrão	Descrição
Sub-rede	Nenhum valor padrão	Especifique a mesma sub-rede da sub-rede preferencial do sistema de arquivos Amazon FSx for NetApp ONTAP. Você pode encontrar o ID de sub-rede preferencial do sistema de arquivos no FSx console da Amazon, na guia Rede e segurança da página de detalhes do sistema FSx de arquivos do ONTAP
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	A versão mais recente da AMI do Amazon Linux 2 em uma determinada Região da AWS.
FSxEndPoint	Nenhum valor padrão	O endereço IP do endpoint de gerenciamento do sistema de arquivos. Você pode encontrar o endereço IP do endpoint de gerenciamento do sistema de arquivos no FSx console da Amazon, na guia Administração da página de detalhes do sistema FSx de arquivos ONTAP.

Parameter	Padrão	Descrição
SecretName	Nenhum valor padrão	AWS Secrets Manager nome secreto contendo a senha do `fsxadmin` usuário do sistema de arquivos. Essa é a senha que você forneceu ao criar o sistema de arquivos.

3. Escolha Próximo.
4. Em Opções, escolha Próximo.
5. Em Análise, analise e confirme as configurações. Você deve selecionar a caixa de seleção confirmando que o modelo cria os recursos do IAM.
6. Selecione Criar para implantar a stack.

Você pode ver o status da pilha no AWS CloudFormation console na coluna Status. Você deverá visualizar um status CREATE_COMPLETE em cerca de cinco minutos.

Fazer login no Grafana

Após a conclusão da implantação, use seu navegador para fazer login no painel da Grafana no IP e na porta 3000 da instância da Amazon EC2 :

```
http://EC2_instance_IP:3000
```

Quando solicitado, use o nome de usuário (`admin`) e a senha (`pass`) padrão do Grafana. Recomendamos que você altere sua senha assim que fizer login.

Para obter mais informações, consulte a página NetApp Harvest em GitHub.

Solução de problemas do Harvest e Grafana

Se você encontrar algum dado ausente mencionado nos painéis do Harvest e do Grafana ou estiver tendo problemas para configurar o Harvest e o Grafana FSx com o ONTAP, verifique os tópicos a seguir para uma possível solução.

Tópicos

- Os painéis de SVM e volume estão em branco
- CloudFormation pilha revertida após o tempo limite

Os painéis de SVM e volume estão em branco

Se a AWS CloudFormation pilha foi implantada com sucesso e puder entrar em contato com a Grafana, mas os painéis de SVM e volume estiverem em branco, use o procedimento a seguir para solucionar problemas em seu ambiente. Você precisará de acesso SSH à EC2 instância da Amazon na qual o Harvest e o Grafana estão implantados.

1. Faça SSH na EC2 instância da Amazon em que seus clientes Harvest e Grafana estão sendo executados.

```
[~]$ ssh ec2-user@ec2_ip_address
```

2. Use o seguinte comando para abrir o arquivo `harvest.yml` e:
   - Verifique se uma entrada foi criada FSx para sua instância do ONTAP como`Cluster-2`.
   - Verifique se as entradas de nome de usuário e senha correspondem às suas credenciais de `fsxadmin`.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/
harvest.yml
```

3. Se o campo de senha estiver em branco, abra o arquivo em um editor e atualize-o com a senha de `fsxadmin` da seguinte forma:

```
[ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
harvest.yml
```

4. Certifique-se de que as credenciais de usuário de `fsxadmin` estejam armazenadas no Secrets Manager no formato a seguir para qualquer implantação futura, substituindo *`fsxadmin_password`* pela sua senha.

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

CloudFormation pilha revertida após o tempo limite

Se você não conseguir implantar a CloudFormation pilha com êxito e ela estiver sendo revertida com erros, use o procedimento a seguir para resolver o problema. Você precisará de acesso SSH à EC2 instância implantada pela pilha CloudFormation .

1. Reimplante a CloudFormation pilha, certificando-se de que a reversão automática esteja desativada.
2. Faça SSH na EC2 instância da Amazon em que seus clientes Harvest e Grafana estão sendo executados.

   ```
   [~]$ ssh ec2-user@ec2_ip_address
   ```

3. Use o comando a seguir para verificar se os contêineres do docker foram iniciados com sucesso.

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
   ```

   Na resposta, você deverá ver cinco contêineres da seguinte forma:

   ```
   CONTAINER ID   IMAGE                  COMMAND                  CREATED
    STATUS                          PORTS                     NAMES
   6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
    Restarting (1) 20 seconds ago                             harvest_cluster-2
   3cf3e3623fde   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago   Up
    About a minute                                            harvest_cluster-1
   708f3b7ef6f8   grafana/grafana         "/run.sh"                8 minutes ago   Up
    8 minutes                   0.0.0.0:3000->3000/tcp   harvest_grafana
   0febee61cab7   prom/alertmanager       "/bin/alertmanager -…"   8
    minutes ago   Up 8 minutes                    0.0.0.0:9093->9093/tcp
    harvest_prometheus_alertmanager
   1706d8cd5a0c   prom/prometheus         "/bin/prometheus --c…"   8 minutes ago   Up
    8 minutes                   0.0.0.0:9090->9090/tcp   harvest_prometheus
   ```

4. Se os contêineres do docker não estiverem em execução, verifique se há falhas no arquivo `/var/log/cloud-init-output.log` da seguinte maneira.

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
        PLAY [Manage Harvest]
    ************************************************************
   ```

```
TASK [Gathering Facts] ***********************************************************
ok: [localhost]

TASK [Verify images] *************************************************************
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
 "changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
 ('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
 "changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP ***********************************************************************
localhost                  : ok=1    changed=0    unreachable=0    failed=1
 skipped=0    rescued=0    ignored=0
```

5. Se houver falhas, execute os comandos a seguir para implantar os contêineres do Harvest e Grafana.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
     [ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml --tags api
```

6. Valide os contêineres iniciados com sucesso executando sudo docker ps e conectando-se ao seu URL do Harvest e Grafana.

Monitoramento FSx de chamadas da API ONTAP com AWS CloudTrail

FSx A Amazon está integrada com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço na Amazon FSx. CloudTrail captura todas as chamadas de FSx API da Amazon para o Amazon FSx for NetApp ONTAP como eventos. As chamadas capturadas incluem chamadas do FSx console da Amazon e de chamadas de código para operações de FSx API da Amazon.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para a Amazon. FSx Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita à Amazon FSx. Você também pode determinar o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

FSx Informações da Amazon em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade da API ocorre na Amazon FSx, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo de eventos em sua AWS conta, incluindo eventos para a Amazon FSx, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as AWS regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS CloudTrail :

- Criando uma trilha para o seu Conta da AWS
- AWS integrações de serviços com CloudTrail o Logs
- Configurando notificações do Amazon SNS para CloudTrail

- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as chamadas de FSx API da Amazon são registradas por CloudTrail. Por exemplo, chamadas para as `TagResource` operações `CreateFileSystem` e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail userIdentity no Guia do AWS CloudTrail usuário.

Entendendo as entradas do arquivo de FSx log da Amazon

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `TagResource` operação quando uma tag para um sistema de arquivos é criada a partir do console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `UntagResource` ação quando uma tag de um sistema de arquivos é excluída do console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
```

```
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

Trabalhando com o Microsoft Active Directory no FSx ONTAP

A Amazon FSx trabalha com o Microsoft Active Directory para se integrar aos seus ambientes existentes. O Active Directory é o serviço de diretório da Microsoft usado para armazenar informações sobre objetos na rede e ajudar administradores e usuários a encontrar e usar essas informações. Esses objetos geralmente incluem recursos compartilhados, como servidores de arquivos e contas de usuários e computadores da rede.

Opcionalmente, você pode unir suas máquinas virtuais FSx de armazenamento do ONTAP (SVMs) ao seu domínio do Active Directory para fornecer autenticação de usuário e controle de acesso em nível de arquivo e pasta. Assim, os clientes do bloco de mensagens do servidor (SMB) podem usar suas identidades de usuário existentes no Active Directory para se autenticar e acessar os volumes de SVM. Seus usuários podem utilizar suas identidades existentes para controlar o acesso a arquivos e pastas individuais. Além disso, você pode migrar seus arquivos e pastas existentes e suas configurações de lista de controle de acesso (ACL) de segurança para a Amazon FSx sem nenhuma modificação.

Se a infraestrutura de domínio do Microsoft Active Directory não estiver disponível, você poderá configurar um servidor Server Message Block (SMB) em um grupo de trabalho em uma SVM como alternativa à associação de uma SVM a um Microsoft Active Directory. Para obter mais informações, consulte Configurando um servidor SMB em um grupo de trabalho.

Ao associar o Amazon FSx for NetApp ONTAP a um Active Directory, você associa o sistema de arquivos SVMs ao Active Directory de forma independente. Isso significa que você pode ter um sistema de arquivos com alguns SVMs que estão associados a um Active Directory e outros SVMs que não estão.

Após a associação de uma SVM a um Active Directory, você pode atualizar as seguintes propriedades de configuração do Active Directory:

- Endereços IP do servidor DNS
- Nome de usuário e senha da conta de serviço do Active Directory autogerenciado

Tópicos

- Pré-requisitos para unir uma SVM a um Microsoft AD autogerenciado

- Práticas recomendadas para trabalhar com o Active Directory
- Como funciona SVMs a adesão ao Microsoft Active Directory
- Como gerenciar configurações do Active Directory para SVM

Pré-requisitos para unir uma SVM a um Microsoft AD autogerenciado

Antes de associar um FSx SVM do ONTAP a um domínio autogerenciado do Microsoft AD, certifique-se de que o Active Directory e a rede atendam aos requisitos descritos nas seções a seguir.

Tópicos

- Requisitos do Active Directory on-premises
- Requisitos de configuração de rede
- Requisitos de conta de serviço do Active Directory

Requisitos do Active Directory on-premises

Verifique se você já tem um Microsoft AD on-premises ou autogerenciado ao qual possa unir a SVM. Esse Active Directory deve ter a seguinte configuração:

- O nível funcional de domínio do controlador de domínios do Active Directory está no Windows Server 2000 ou posterior.
- O Active Directory usa um nome de domínio que não está no formato de domínio de rótulo único (SLD). A Amazon FSx não oferece suporte a domínios SLD.
- Se você tiver sites do Active Directory definidos, certifique-se de que as sub-redes na VPC associadas ao seu sistema de arquivos FSx for ONTAP estejam definidas nos mesmos sites do Active Directory e que não existam conflitos entre as sub-redes da VPC e as sub-redes nos sites do Active Directory.

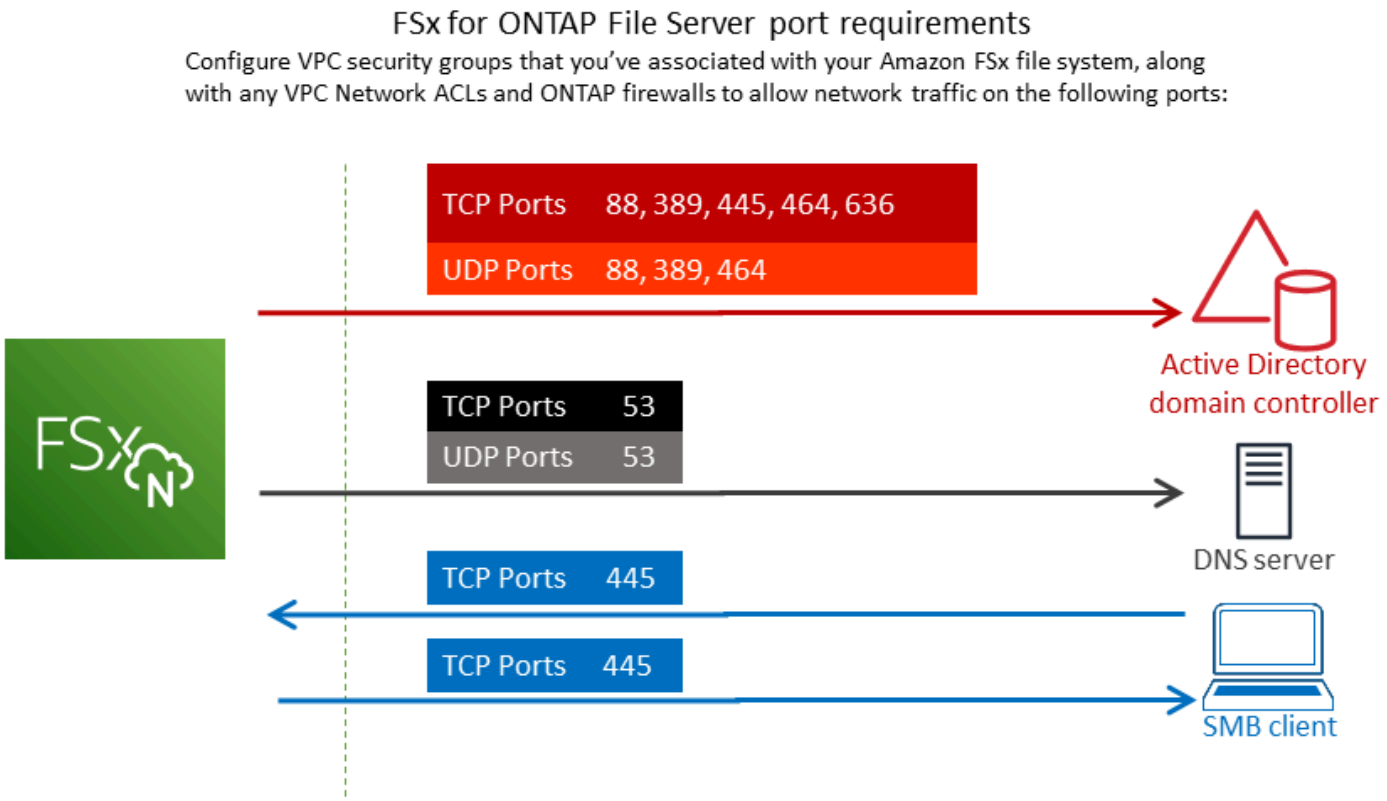
> **Note**
>
> Se você estiver usando AWS Directory Service, o FSx for ONTAP não suporta SVMs a adesão ao Simple Active Directory.

Requisitos de configuração de rede

Confira se você tem as configurações de rede a seguir e as informações associadas disponíveis para você.

> **Important**
>
> Para que uma SVM ingresse no Active Directory, você precisa garantir que as portas documentadas neste tópico permitam tráfego entre todos os controladores de domínio do Active Directory e os dois endereços IP iSCSI (interfaces lógicas iscsi_1 e iscsi_2 ()) na SVM. LIFs

- Os endereços IP do servidor DNS e do controlador de domínios do Active Directory.
- Conectividade entre a Amazon VPC em que você está criando o sistema de arquivos e o Active Directory autogerenciado usando AWS Direct Connect, AWS VPN ou AWS Transit Gateway.
- O grupo de segurança e a rede ACLs VPC das sub-redes nas quais você está criando o sistema de arquivos devem permitir o tráfego nas portas e nas direções mostradas no diagrama a seguir.



A função de cada porta é descrita na tabela a seguir.

Protocolo	Portas	Função
TCP/UDP	53	Domain Name System (DNS)
TCP/UDP	88	Autenticação de Kerberos
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)
TCP	445	Compartilhamento de arquivos de SMB para serviços de diretório
TCP/UDP	464	Alterar/definir senha
TCP	636	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)

- Essas regras de tráfego também devem ser espelhadas nos firewalls que se aplicam a cada um dos controladores de domínio, servidores DNS, clientes e administradores do Active Directory. FSx FSx

> **Important**
>
> Embora os grupos de segurança da Amazon VPC exijam que as portas sejam abertas somente na direção em que o tráfego de rede é iniciado, a maioria dos firewalls do Windows e da rede VPC ACLs exigem que as portas sejam abertas em ambas as direções.

Requisitos de conta de serviço do Active Directory

Confira se você tem uma conta de serviço em seu Microsoft AD autogerenciado, com permissões delegadas para unir computadores ao domínio. Uma conta de serviço é uma conta de usuário no Active Directory autogerenciado que recebeu a delegação de certas tarefas.

No mínimo, as seguintes permissões devem ser delegadas à conta de serviço na UO à qual você está unindo a SVM:

- Capacidade de redefinir senhas
- Capacidade de restringir contas de ler e gravar dados
- Capacidade de definir a propriedade `msDS-SupportedEncryptionTypes` em objetos de computador
- Capacidade validada para gravar no nome do host DNS
- Capacidade validada para gravar no nome da entidade principal de serviço
- Capacidade para criar e excluir objetos de computador
- Capacidade validada para ler e gravar restrições de conta

Elas representam o conjunto mínimo de permissões necessárias para associar objetos de computador ao Active Directory. Para obter mais informações, consulte o tópico da documentação do Windows Server Erro: o acesso é negado quando usuários não administradores que receberam controle delegado tentam unir computadores a um controlador de domínio.

Para saber mais sobre como criar uma conta de serviço com as permissões corretas, consulte Delegando permissões à sua conta de FSx serviço da Amazon.

> **Important**
>
> A Amazon FSx exige uma conta de serviço válida durante toda a vida útil do seu sistema de FSx arquivos Amazon. A Amazon FSx deve ser capaz de gerenciar totalmente o sistema de arquivos e realizar tarefas que exijam que ela desassocie e reuna recursos ao seu domínio do Active Directory. Essas tarefas incluem a substituição de um sistema de arquivos ou SVM com falha ou a correção do software NetApp ONTAP. Mantenha suas informações de configuração do Active Directory atualizadas com a Amazon FSx, incluindo as credenciais da conta de serviço. Para saber mais, consulte Mantendo sua configuração do Active Directory atualizada com a Amazon FSx.

Se esta é sua primeira vez usando AWS e FSx para o ONTAP, certifique-se de concluir as etapas iniciais de configuração antes de iniciar sua integração com o Active Directory. Para obter mais informações, consulte Configurando o FSx ONTAP.

> **Important**
>
> Não mova objetos de computador que a Amazon FSx cria na OU após sua SVMs criação, nem exclua seu Active Directory enquanto sua SVM estiver associada a ele. Fazer isso fará com que seu SVMs seja configurado incorretamente.

Práticas recomendadas para trabalhar com o Active Directory

Aqui estão algumas sugestões e diretrizes que você deve considerar ao associar o Amazon FSx for NetApp ONTAP SVMs ao seu Microsoft Active Directory autogerenciado. Observe que elas são práticas recomendadas, mas não obrigatórias.

Delegando permissões à sua conta de FSx serviço da Amazon

Certifique-se de configurar a conta de serviço que você fornece à Amazon FSx com as permissões mínimas necessárias. Além disso, separe a unidade organizacional (UO) de outras preocupações do controlador de domínio.

Para associar FSx SVMs a Amazon ao seu domínio, certifique-se de que a conta de serviço tenha permissões delegadas. Os membros do grupo Administradores de domínio têm permissões suficientes para realizar essa tarefa. No entanto, como prática recomendada, use uma conta de serviço que tenha apenas as permissões mínimas necessárias para fazer isso. O procedimento a seguir demonstra como delegar somente as permissões necessárias FSx para ingressar no ONTAP em SVMs seu domínio.

Execute este procedimento em uma máquina que esteja associada ao seu diretório e tenha instalado o snap-in do MMC Active Directory User and Computers.

Para criar uma conta de serviço para seu domínio do Microsoft Active Directory

1. Verifique se você está conectado como administrador de domínio para o domínio do Microsoft Active Directory.
2. Abra o snap-in do MMC de Computadores e Uuários do Active Directory.
3. No painel de tarefas, expanda o nó do domínio.
4. Localize e abra o menu de contexto (clique com o botão direito do mouse) na UO que deseja modificar e selecione Delegar controle.
5. Na página Assistente de delegação de controle, escolha Próximo.

6. Escolha Adicionar para adicionar um usuário específico ou um grupo específico em Usuários e grupos selecionados e selecione Próximo.
7. Na página Tasks to Delegate (Tarefas para delegar), selecione Create a custom task to delegate (Criar uma tarefa personalizada para delegar) e, em seguida, selecione Next (Avançar).
8. Escolha Somente os objetos a seguir na pasta, e depois Objetos de computador.
9. Selecione Criar objetos selecionados nesta pasta e Excluir objetos selecionados nesta pasta. Escolha Próximo.
10. Em Mostrar essas permissões, verifique se Geral e Específico da propriedade estão selecionados.
11. Em Permissões, escolha o seguinte:

    - Redefinir senha
    - Restrições de leitura e gravação da conta
    - Gravação validada no nome do host DNS
    - Gravação validada no nome da entidade principal do serviço
    - Escreva MSDs- SupportedEncryptionTypes
12. Escolha Next (Próximo) e, em seguida, escolha Finish (Concluir).
13. Feche o snap-in do MMC de Computadores e Usuários do Active Directory.

> **Important**
>
> Não mova objetos de computador que a Amazon FSx cria na OU após sua SVMs criação. Isso fará com que seu SVMs seja configurado incorretamente.

Mantendo sua configuração do Active Directory atualizada com a Amazon FSx

Para uma disponibilidade ininterrupta de sua Amazon FSx SVMs, atualize a configuração autogerenciada do Active Directory (AD) de uma SVM ao alterar sua configuração autogerenciada do AD.

Por exemplo, suponha que o seu AD use uma política de redefinição de senha baseada em tempo. Nesse caso, assim que a senha for redefinida, certifique-se de atualizar a senha da conta de serviço na Amazon FSx. Para fazer isso, use o FSx console da Amazon, a FSx API da Amazon ou AWS

CLI. Da mesma forma, se os endereços IP do servidor DNS mudarem para seu domínio do Active Directory, assim que a alteração ocorrer, atualize os endereços IP do servidor DNS com a Amazon. FSx

Se houver um problema com a configuração atualizada do AD autogerenciado, o estado da SVM mudará para Configuração incorreta. Esse estado mostra uma mensagem de erro e uma ação recomendada ao lado da descrição da SVM no console, na API e na CLI. Se ocorrer um problema com a configuração do AD da SVM, certifique-se de seguir a ação corretiva recomendada para as propriedades de configuração. Se o problema for resolvido, verifique se o estado da SVM muda para Criado.

Para ter mais informações, consulte Atualizando as configurações existentes do SVM Active Directory usando a API AWS Management Console, AWS CLI, e e Modificar uma configuração do Active Directory usando a CLI do ONTAP.

Como usar grupos de segurança para limitar o tráfego na VPC

Para limitar o tráfego de rede na nuvem privada virtual (VPC), você pode implementar o princípio do privilégio mínimo na VPC. Em outras palavras, você pode limitar as permissões ao mínimo necessário. Para isso, use as regras do grupo de segurança. Para saber mais, consulte Grupos de segurança da Amazon VPC.

Como criar regras de saída de grupo de segurança para a interface de rede do sistema de arquivos

Para maior segurança, considere configurar um grupo de segurança com regras de tráfego de saída. Essas regras devem permitir o tráfego de saída somente para os controladores de domínios do AD autogerenciado ou dentro da sub-rede ou do grupo de segurança. Aplique esse grupo de segurança à VPC associada à interface de rede elástica do seu sistema de FSx arquivos Amazon. Para saber mais, consulte Controle de acesso ao sistema de arquivos com a Amazon VPC.

Como funciona SVMs a adesão ao Microsoft Active Directory

Sua organização pode gerenciar identidades e dispositivos usando um Active Directory, seja on-premises ou na nuvem. Com FSx o ONTAP, você pode SVMs associá-lo diretamente ao seu domínio existente do Active Directory das seguintes maneiras:

- Ingressar SVMs em um novo Active Directory na criação:

  - Usando a opção de criação padrão no FSx console da Amazon para criar um novo sistema de arquivos FSx para o ONTAP, você pode unir o SVM padrão a um Active Directory autogerenciado. Para obter mais informações, consulte Criar um sistema de arquivos (console).
  - Usando o FSx console da Amazon ou a FSx API da Amazon para criar uma nova SVM em um sistema de arquivos existente FSx para ONTAP. AWS CLI Para obter mais informações, consulte Criar máquinas virtuais de armazenamento (SVM).
- Unindo SVMs o existente a um Active Directory:
  - Usando a API AWS Management Console AWS CLI, e para unir uma SVM a um Active Directory e tentar unir novamente uma SVM a um Active Directory se a tentativa inicial de associação falhar. Você também pode atualizar algumas propriedades de configuração do Active Directory para SVMs aquelas que já estão associadas a um Active Directory. Para obter mais informações, consulte Como gerenciar configurações do Active Directory para SVM.
  - Usando a CLI do NetApp ONTAP ou a API REST para unir, tentar unir e desassociar novamente as configurações do SVM Active Directory. Para obter mais informações, consulte Atualizando as configurações do SVM Active Directory usando a CLI NetApp .

> **Important**
>
> - A Amazon FSx só registra registros DNS para uma SVM se você usar o Microsoft DNS como o serviço DNS padrão. Se você usa um DNS de terceiros, você deve configurar entradas de DNS manualmente para sua Amazon FSx SVMs depois de criá-las.
> - Se você usa AWS Managed Microsoft AD, você deve especificar um grupo como Administradores AWS Delegados, FSx Administradores AWS Delegados ou um grupo personalizado com permissões delegadas para a OU.

Quando você associa uma FSx SVM do ONTAP diretamente a um Active Directory autogerenciado, a SVM reside na mesma floresta do Active Directory (o contêiner lógico mais alto em uma configuração do Active Directory que contém domínios, usuários e computadores) e no mesmo domínio do Active Directory que seus usuários e recursos existentes, incluindo servidores de arquivos existentes.

Informações necessárias ao unir uma SVM a um Active Directory

É necessário fornecer as seguintes informações sobre seu Active Directory ao associar uma SVM a um Active Directory, independentemente da operação de API escolhida:

- O Nome NetBIOS do objeto de computador do Active Directory que será criado para a SVM. Trata-se do nome da SVM no Active Directory, que deve ser exclusivo no Active Directory. Não use o nome NetBIOS do domínio inicial. O nome NetBIOS não pode ter mais de 15 caracteres.
- O nome de domínio totalmente qualificado (FQDN) do Active Directory. O FQDN não pode ter mais de 255 caracteres.

  > **Note**
  >
  > O FQDN não pode estar no formato de domínio de rótulo único (SLD). A Amazon FSx não oferece suporte a domínios SLD.

- Até três endereços IP dos servidores DNS ou dos hosts do domínio.

  Os endereços IP do servidor DNS e do controlador de domínios do Active Directory podem estar em qualquer intervalo de endereços IP, exceto:

  - endereços IP que entram em conflito com aqueles de propriedade da Amazon Web Services nessa Região da AWS. Para obter uma lista de endereços AWS IP por região, consulte os intervalos de endereços AWS IP.
  - Endereços IP no seguinte intervalo de blocos CIDR: 198.19.0.0/16

- Nome de usuário e senha de uma conta de serviço em seu domínio do Active Directory para FSx a Amazon usar ao unir o SVM ao domínio do Active Directory. Para obter mais informações sobre requisitos de conta de serviço, consulte Requisitos de conta de serviço do Active Directory.
- (Opcional) A Unidade Organizacional (UO) no domínio ao qual você une a SVM.

  > **Note**
  >
  > Se você unir sua SVM a um AWS Directory Service Active Directory, deverá fornecer uma OU que esteja dentro da OU padrão AWS Directory Service criada para os objetos de diretório relacionados a. AWS Isso ocorre porque o AWS Directory Service não fornece acesso à `Computers` OU padrão do Active Directory. Por exemplo, se o

domínio do Active Directory for `example.com`, você poderá especificar a seguinte UO: `OU=Computers,OU=example,DC=example,DC=com`.

- (Opcional) O grupo de domínio ao qual você está delegando autoridade para executar ações administrativas em seu sistema de arquivos. Por exemplo, esse grupo de domínio pode gerenciar compartilhamentos de arquivos SMB do Windows, assumir a propriedade de arquivos e pastas e assim por diante. Se você não especificar esse grupo, a Amazon FSx delegará essa autoridade ao grupo Administradores de Domínio em seu domínio do Active Directory por padrão.

Como gerenciar configurações do Active Directory para SVM

Esta seção descreve como usar a FSx API AWS Management Console, AWS CLI, e a CLI ONTAP para fazer o seguinte:

- Associar uma SVM existente a um Active Directory
- Modificar a configuração de Active Directory de uma SVM existente
- Removendo SVMs de um Active Directory

Para remover uma SVM de um Active Directory, você deve usar a NetApp CLI do ONTAP.

Tópicos

- Ingressando SVMs no Active Directory usando a API AWS Management Console, AWS CLI e
- Atualizando as configurações existentes do SVM Active Directory usando a API AWS Management Console, AWS CLI, e
- Atualizando as configurações do SVM Active Directory usando a CLI NetApp

Ingressando SVMs no Active Directory usando a API AWS Management Console, AWS CLI e

Aplique o procedimento a seguir para associar uma SVM existente a um Active Directory. Nesse procedimento, a SVM ainda não está associada a um Active Directory.

Para associar uma SVM a um Active Directory (AWS Management Console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.

2. Escolha a SVM que deseja associar a um Active Directory:

   - No painel de navegação à esquerda, escolha Sistemas de arquivos e, em seguida, escolha o sistema de arquivos do ONTAP com a SVM que você deseja atualizar.
   - Escolha a guia Máquinas virtuais de armazenamento.

     Ou

   - Para exibir uma lista de todos os disponíveis SVMs, no painel de navegação esquerdo, expanda ONTAP e escolha Armazenamento de máquinas virtuais. Uma lista de tudo SVMs em sua conta no Região da AWS é exibida.

   Selecione na lista a SVM que deseja associar a um Active Directory.
3. No canto superior direito do painel Resumo da SVM, escolha Ações > Ingressar/atualizar o Active Directory. A janela Integrar a SVM a um Active Directory é exibida.
4. Insira as seguintes informações para o Active Directory ao qual você está associando a SVM:

   - O Nome NetBIOS do objeto de computador do Active Directory que será criado para a SVM. Trata-se do nome da SVM no Active Directory, que deve ser exclusivo no Active Directory. Não use o nome NetBIOS do domínio inicial. O nome NetBIOS não pode ter mais de 15 caracteres.
   - O nome de domínio totalmente qualificado (FQDN) do Active Directory. O nome do domínio não pode ter mais de 255 caracteres.
   - Endereços IP do servidor DNS — Os IPv4 endereços dos servidores DNS do seu domínio.
   - Nome de usuário da conta de serviço: o nome de usuário da conta de serviço no seu Active Directory existente. Não inclua um prefixo ou sufixo de domínio. Por exemplo, para `EXAMPLE\ADMIN`, use apenas `ADMIN`.
   - Senha da conta de serviço: a senha da conta de serviço.
   - Confirmar senha: a senha da conta de serviço.
   - (Opcional) Unidade organizacional (UO): o nome do caminho distinto da unidade organizacional à qual você deseja unir sua SVM.
   - Grupo de administradores delegado do sistema de arquivos: o nome do grupo no Active Directory que pode administrar o sistema de arquivos.

Se você estiver usando AWS Managed Microsoft AD, deverá especificar um grupo como Administradores AWS Delegados, FSx Administradores AWS Delegados ou um grupo personalizado com permissões delegadas à OU.

Se você estiver fazendo a associação com um Active Directory autogerenciado, use o nome do grupo em seu Active Directory. O grupo padrão é `Domain Admins`.

5. Escolha Ingressar no Active Directory para associar a SVM ao Active Directory usando a configuração que você forneceu.

Para unir uma SVM a um Active Directory (AWS CLI)

- Para unir um FSx for ONTAP SVM a um Active Directory, use o comando update-storage-virtual-machineCLI (ou a operação de UpdateStorageVirtualMachineAPI equivalente), conforme mostrado no exemplo a seguir.

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
\
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Depois de criar com sucesso a máquina virtual de armazenamento, a Amazon FSx retorna sua descrição no formato JSON, conforme mostrado no exemplo a seguir.

```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
```

```
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],

  }
}
```

Atualizando as configurações existentes do SVM Active Directory usando a API AWS Management Console, AWS CLI, e

Aplique o procedimento a seguir para atualizar a configuração do Active Directory de uma SVM que já está associada a um Active Directory.

Para atualizar a configuração de Active Directory para uma SVM (AWS Management Console)

1. Abra o FSx console da Amazon em https://console.aws.amazon.com/fsx/.
2. Escolha a SVM a ser atualizada da seguinte forma:

   - No painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema de arquivos do ONTAP com a SVM que você deseja atualizar.
   - Escolha a guia Máquinas virtuais de armazenamento.

     Ou

   - Para exibir uma lista de todos os SVMs disponíveis, no painel de navegação esquerdo, expanda ONTAP e escolha Armazenamento de máquinas virtuais.

   Selecione a SVM que você deseja atualizar na lista.
3. No painel Resumo da SVM, escolha Ações > Ingressar/atualizar o Active Directory. A janela Atualizar a configuração do Active Directory da SVM é exibida.
4. Você pode atualizar as seguintes propriedades de configuração do Active Directory nessa janela.

   - Endereços IP do servidor DNS — Os IPv4 endereços dos servidores DNS do seu domínio.
   - Nome de usuário da conta de serviço: o nome de usuário da conta de serviço em seu Active Directory existente. Não inclua um prefixo ou sufixo de domínio. Para `EXAMPLE\ADMIN`, use `ADMIN`.
   - Senha da conta de serviço: a senha da conta de serviço do Active Directory.
5. Depois de informar suas atualizações, escolha Atualizar o Active Directory para fazer as alterações.

Aplique o procedimento a seguir para atualizar a configuração do Active Directory de uma SVM que já está associada a um Active Directory.

Para atualizar a configuração de Active Directory para uma SVM (AWS CLI)

- Para atualizar a configuração do Active Directory de uma SVM com a API AWS CLI ou, use o comando update-storage-virtual-machineCLI (ou a operação de API UpdateStorageVirtualMachineequivalente), conforme mostrado no exemplo a seguir.

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-abcdef0123456789a\
    --active-directory-configuration \
    SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}'
```

Atualizando as configurações do SVM Active Directory usando a CLI NetApp

Você pode usar a CLI do NetApp ONTAP para unir e desassociar sua SVM a um Active Directory e para modificar uma configuração existente do SVM Active Directory.

Associar uma SVM a um Active Directory usando a CLI do ONTAP

Você pode unir os existentes SVMs a um Active Directory usando a CLI do ONTAP, conforme descrito no procedimento a seguir. É possível fazer isso mesmo que a SVM já esteja associada a um Active Directory.

1. Para acessar o ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o seguinte comando. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.
2. Crie uma entrada de DNS do Active Directory fornecendo o nome DNS completo do diretório (`corp.example.com`) e pelo menos um endereço IP do servidor DNS.

   ```
   ::>vserver services name-service dns create -vserver svm_name -
   domains corp.example.com -name-servers dns_ip_1, dns_ip_2
   ```

Para verificar a conexão com os servidores DNS, execute o comando a seguir. *svm_name*Substitua por suas próprias informações.

```
FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name

                            Name Server
Vserver       Name Server     Status       Status Details
------------- --------------- ------------ --------------------------
svm_name      172.31.14.245   up           Response time (msec): 0
svm_name      172.31.25.207   up           Response time (msec): 1
2 entries were displayed.
```

3. Para unir a SVM ao Active Directory, execute o comando a seguir. Observe que você deverá especificar um `computer_name` que ainda não exista no Active Directory e fornecer o nome DNS do diretório para o `-domain`. Para`-OU`, insira o OUs que você deseja que o SVM participe, bem como o nome DNS completo no formato DC.

```
::>vserver cifs create -vserver svm_name -cifs-server computer_name -
domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
```

Para verificar o status da conexão do Active Directory, execute o seguinte comando:

```
::>vserver cifs check -vserver svm_name

              Vserver : svm_name
                    Cifs NetBIOS Name : svm_netBIOS_name
                          Cifs Status : Running
                                 Site : Default-First-Site-Name
Node Name       DC Server Name  DC Server IP    Status   Status Details
--------------- --------------  --------------- ------   --------------
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245   up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245   up       Response time (msec): 20
2 entries were displayed.
```

4. Se você não conseguir acessar compartilhamentos após essa junção, determine se a conta que você está usando para acessar o compartilhamento tem permissões. Por exemplo, se você

estiver usando a `Admin` conta padrão (um administrador delegado) com um Active Directory AWS gerenciado, deverá executar o seguinte comando no ONTAP. O `netbios_domain` corresponde ao nome de domínio do Active Directory (para`corp.example.com`, o `netbios_domain` usado aqui é`example`).

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
 svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

Modificar uma configuração do Active Directory usando a CLI do ONTAP

Você pode usar a CLI do ONTAP para modificar uma configuração existente do Active Directory.

1. Para acessar o ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Execute o comando a seguir para derrubar temporariamente o servidor CIFS da SVM:

   ```
   FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
   ```

3. Se precisar modificar as entradas de DNS do Active Directory, execute o seguinte comando:

   ```
   ::>vserver services name-service dns modify -vserver svm_name -
   domains corp.example.com -name-servers dns_ip_1,dns_ip_2
   ```

   Você pode validar o status da conexão com os servidores DNS do Active Directory usando o comando `vserver services name-service dns check -vserver svm_name`.

   ```
   ::>vserver services name-service dns check -vserver svm_name
                               Name Server
   Vserver       Name Server     Status       Status Details
   ------------- --------------- ------------ --------------------------
   svmciad       dns_ip_1        up           Response time (msec): 1
   svmciad       dns_ip_2        up           Response time (msec): 1
   ```

```
2 entries were displayed.
```

4. Se você precisar modificar a própria configuração do Active Directory, poderá alterar os campos existentes usando o seguinte comando, substituindo:

   - *computer_name*, se você quiser modificar o nome NetBIOS (conta da máquina) do SVM.
   - *domain_name*, se você quiser modificar o nome do domínio. Isso deverá corresponder à entrada do domínio do DNS anotada na Etapa 3 desta seção (`corp.example.com`).
   - `organizational_unit`, se você quiser modificar UO (`OU=Computers,OU=example,DC=corp,DC=example,DC=com`).

   Você precisará inserir novamente as credenciais do Active Directory que usou para associar esse dispositivo ao Active Directory.

   ```
   ::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
   domain domain_name -OU organizational_unit
   ```

   Você poderá verificar o status da conexão do Active Directory usando o comando `vserver cifs check -vserver` *svm_name*.

5. Quando terminar de modificar a configuração do Active Directory e do DNS, reinicie o servidor CIFS executando o seguinte comando:

   ```
   ::>vserver cifs modify -vserver svm_name -status-admin up
   ```

Desassocie um Active Directory do seu SVM usando a CLI do NetApp ONTAP

A CLI do NetApp ONTAP também pode ser usada para desassociar seu SVM de um Active Directory seguindo as etapas abaixo:

1. Para acessar o ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o seguinte comando. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Exclua o servidor CIFS que desassociou o dispositivo do Active Directory executando o comando a seguir. Para que o ONTAP exclua a conta da máquina da SVM, forneça as credenciais que você usou originalmente para associar a SVM ao Active Directory.

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Se precisar modificar as entradas de DNS do Active Directory, execute o seguinte comando:

```
FsxId0123456789a::vserver cifs delete -vserver svm_name

In order to delete an Active Directory machine account for the CIFS server, you
 must supply the name and password of a Windows account with
sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

Enter the user name: user_name

Enter the password:

Warning: There are one or more shares associated with this CIFS server
         Do you really want to delete this CIFS server and all its shares? {y|n}: y
```

4. Exclua os servidores DNS do Active Directory executando o seguinte comando:

```
::vserver services name-service dns delete -vserver svm_name
```

Se você receber um aviso como o seguinte, indicando que o `dns` deve ser removido como `ns-switch`, e não planejar associar novamente esse dispositivo a um Active Directory, será possível remover as entradas `ns-switch`.

```
Warning: "DNS" is present as one of the sources in one or more ns-switch databases
 but no valid DNS configuration was found for Vserver
         "svm_name". Remove "DNS" from ns-switch using the "vserver services name-
service ns-switch" command. Configuring "DNS" as a source
         in the ns-switch setting when there is no valid configuration can cause
 protocol access issues.
```

5. (Opcional) Remova as entradas `ns-switch` do `dns` executando o comando a seguir. Verifique a ordem de fontes e, em seguida, remova a entrada `dns` do banco de dados `hosts` modificando as `sources` para que elas contenham apenas as outras fontes listadas. Neste exemplo, a única outra fonte é `files`.

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts

                    Vserver: svm_name
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

6. (Opcional) Remova a entrada dns modificando as sources para que o host do banco de dados inclua apenas files.

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

Migrando para a Amazon FSx para ONTAP NetApp

As seções a seguir fornecem informações sobre como migrar seus sistemas de arquivos NetApp ONTAP existentes FSx para a Amazon for NetApp ONTAP.

> **Note**
>
> Se você planeja usar a política de divisão em níveis `All` para migrar seus dados para o nível do grupo de capacidade, tenha em mente que os metadados do arquivo são sempre armazenados no nível SSD e que todos os novos dados do usuário são gravados primeiro no nível SSD. Quando os dados são gravados no nível SSD, o processo de divisão em níveis em segundo plano começa a dividir seus dados no armazenamento do grupo de capacidade, mas esse processo não é imediato e consome recursos da rede. É necessário dimensionar seu nível SSD para contabilizar os metadados do arquivo (de 3 a 7% do tamanho dos dados do usuário), como um buffer para os dados do usuário, antes de serem divididos em níveis no armazenamento do grupo de capacidade. Recomendamos que não exceda 80% de utilização do nível SSD.
> Ao migrar dados, monitore sua camada de SSD usando métricas do sistema de CloudWatch arquivos para garantir que ela não seja preenchida mais rápido do que o processo de hierarquização pode mover os dados para o armazenamento do pool de capacidade.

Tópicos

- Migrando FSx para o ONTAP usando NetApp SnapMirror
- Migrando FSx para o ONTAP usando AWS DataSync

Migrando FSx para o ONTAP usando NetApp SnapMirror

Você pode migrar seus sistemas de arquivos NetApp ONTAP para a Amazon FSx para uso do NetApp ONTAP. NetApp SnapMirror

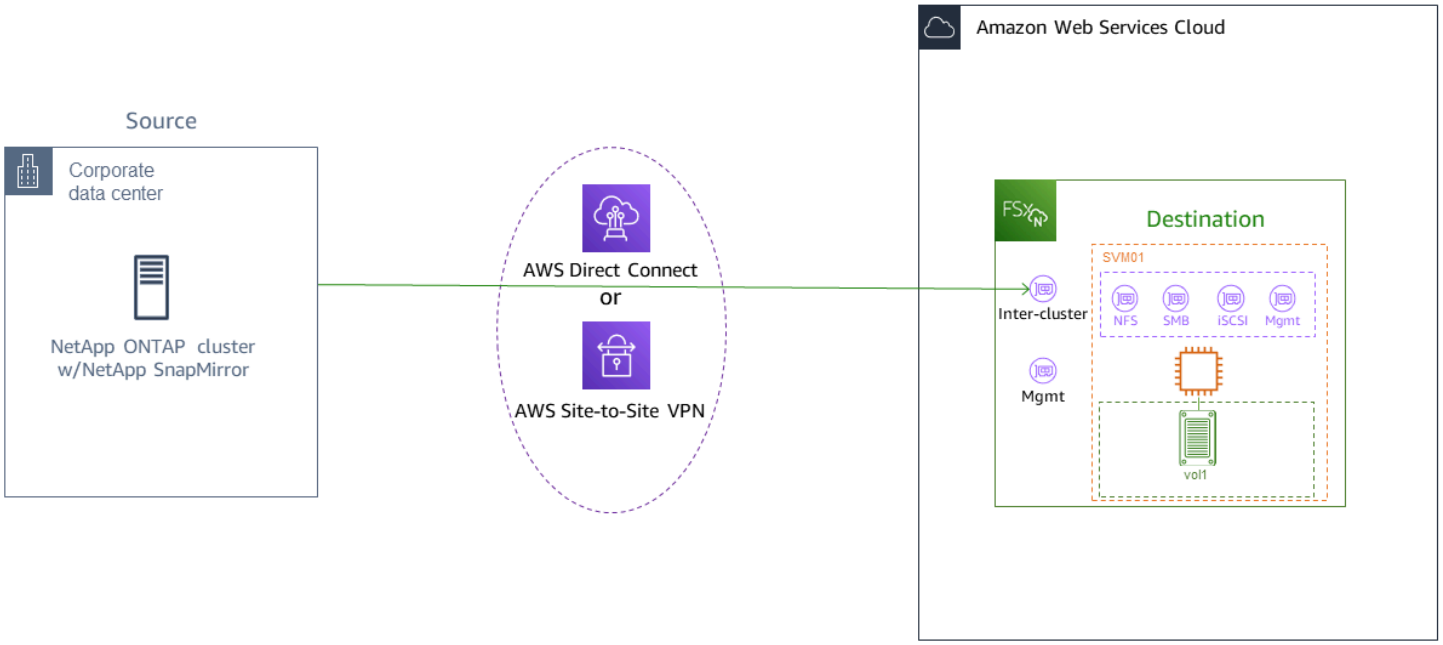
NetApp SnapMirror emprega replicação em nível de bloco entre dois sistemas de arquivos ONTAP, replicando dados de um volume de origem especificado para um volume de destino. Recomendamos usar SnapMirror para migrar sistemas de arquivos ONTAP locais para o NetApp ONTAP. FSx NetApp SnapMirrorA replicação em nível de bloco é rápida e eficiente até mesmo para sistemas de arquivos com:

- Estruturas complexas de diretórios
- Mais de 50 milhões de arquivos
- Arquivos muito pequenos (da ordem de kilobytes)

Quando você costuma migrar SnapMirror FSx para o ONTAP, os dados desduplicados e compactados permanecem nesses estados, o que reduz os tempos de transferência e reduz a quantidade de largura de banda necessária para a migração. Os snapshots que existem nos volumes do ONTAP de origem são preservados quando migrados para os volumes de destino. A migração de seus sistemas de arquivos NetApp ONTAP locais FSx para o ONTAP envolve as seguintes tarefas de alto nível:

1. Crie o volume de destino na Amazon FSx.
2. Reúna interfaces lógicas de origem e destino (LIFs).
3. Estabelecer o emparelhamento de cluster entre os sistemas de arquivos de origem e destino.
4. Criar um relacionamento de emparelhamento com a SVM.
5. Crie o SnapMirror relacionamento.
6. Manter um cluster de destino atualizado.
7. Vá para o seu sistema FSx de arquivos ONTAP.

O diagrama a seguir ilustra o cenário de migração descrito nesta seção.



Tópicos

- Antes de começar
- Criar o volume de destino
- Registre a origem e o destino entre clusters LIFs
- Estabelecer o emparelhamento de clusters entre a origem e o destino
- Criar um relacionamento de emparelhamento entre SVMs
- Crie o SnapMirror relacionamento
- Transfira dados para o seu sistema FSx de arquivos para ONTAP
- Passando para a Amazon FSx

Antes de começar

Antes de começar a usar os procedimentos descritos nas próximas seções, verifique se você atende aos pré-requisitos a seguir.

- FSx for ONTAP prioriza o tráfego do cliente em relação às tarefas em segundo plano, incluindo armazenamento de dados em camadas, eficiência de armazenamento e backups. Ao migrar dados, e como prática recomendada geral, recomendamos que monitore a capacidade do nível SSD para garantir que não exceda 80% de utilização. Você pode monitorar a utilização do seu nível de SSD usando métricas do sistema de CloudWatch arquivos. Para obter mais informações, consulte Métricas de volume.
- Se você definir a política de divisão de dados em níveis do volume de destino para `All` ao migrar seus dados, todos os metadados do arquivo serão armazenados no nível de armazenamento SSD principal. Os metadados do arquivo são sempre armazenados no nível SSD principal, independentemente da política de divisão de dados em níveis do volume. Recomendamos assumir uma proporção de 1 : 10 para o nível principal : capacidade de armazenamento do nível do grupo de capacidade.
- Os sistemas de arquivos de origem e destino estão conectados na mesma VPC ou em redes que são emparelhadas usando Amazon VPC Peering, Transit Gateway ou. AWS Direct Connect AWS VPN Para obter mais informações, consulte Acessando dados de dentro do Nuvem AWS e O que é emparelhamento de VPC? no Guia de emparelhamento da Amazon VPC.
- O grupo de segurança VPC FSx para o sistema de arquivos ONTAP tem regras de entrada e saída que permitem ICMP e TCP nas portas 443, 10000, 11104 e 11105 para seus endpoints entre clusters (). LIFs

- Verifique se os volumes de origem e destino estão executando versões compatíveis do NetApp ONTAP antes de criar uma relação de proteção de SnapMirror dados. Para obter mais informações, consulte Versões compatíveis do ONTAP para SnapMirror relacionamentos na documentação do usuário NetApp do ONTAP. Os procedimentos apresentados aqui usam um sistema de arquivos NetApp ONTAP local para a fonte.
- Seu sistema de arquivos NetApp ONTAP local (de origem) inclui uma SnapMirror licença.
- Você criou um destino FSx para o sistema de arquivos ONTAP com uma SVM, mas não criou um volume de destino. Para obter mais informações, consulte Criar sistemas de arquivos.

Os comandos nesses procedimentos usam os aliases de cluster, SVM e volume a seguir.

- *FSx-Dest*— o ID do cluster de destino (FSx) (no formato FSx IDABCDEF1234567890a).
- *OnPrem-Source*: o ID do cluster de origem.
- *DestSVM*: o nome da SVM de destino.
- *SourceSVM*: o nome da SVM de origem.
- O nome do volume de origem e o de destino é `vol1`.

> **Note**
>
> Um sistema de arquivos FSx for ONTAP é chamado de cluster em todos os comandos da CLI do ONTAP.

Os procedimentos nesta seção usam os seguintes comandos da CLI do NetApp ONTAP.

- comando volume create
- comandos cluster
- comandos vserver peer
- comandos snapmirror

Você usará a CLI do NetApp ONTAP para criar e gerenciar SnapMirror uma configuração no FSx seu sistema de arquivos do ONTAP. Para obter mais informações, consulte Usar o NetApp ONTAP CLI.

Criar o volume de destino

Você pode criar um volume de destino de proteção de dados (DP) usando o FSx console da Amazon, o AWS CLI e a FSx API da Amazon, além da NetApp CLI e da API REST do ONTAP. Para obter informações sobre a criação de um volume de destino usando o FSx console da Amazon AWS CLI, consulteComo criar volumes.

> **Note**
>
> ONTAP não preserva as economias de compactação pós-processamento obtidas na origem no volume DP de destino quando a política de classificação em camadas do volume de destino é. `All` Para preservar a economia de compactação pós-processamento, você deve definir a política de classificação por níveis de volume de destino como `Auto` e permitir que o sistema de arquivos de destino reaplique a economia de compactação pós-processo inactive-data-compression no destino.

No procedimento a seguir, você usará a CLI do NetApp ONTAP para criar um volume de destino no FSx seu sistema de arquivos for ONTAP. Você precisará da senha de `fsxadmin` e do endereço IP ou nome DNS da porta de gerenciamento do sistema de arquivos.

1. Estabeleça uma sessão SSH com o sistema de arquivos de destino utilizando o usuário e a senha de `fsxadmin` definidos ao criar o sistema de arquivos.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Crie um volume no cluster de destino que tenha uma capacidade de armazenamento que seja, no mínimo, igual à capacidade de armazenamento do volume de origem. Use `-type DP` para designá-lo como destino para um SnapMirror relacionamento.

   Se você planeja usar a divisão de dados em níveis, recomendamos que defina a `-tiering-policy` como `all`. Isso garante que seus dados sejam imediatamente transferidos para o armazenamento do grupo de capacidade e evita que você fique sem capacidade no nível SSD. Após a migração, você pode mudar a `-tiering-policy` para `auto`.

> **Note**
>
> Os metadados do arquivo são sempre armazenados no nível SSD principal, independentemente da política de divisão de dados em níveis do volume.

```
FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
type DP -tiering-policy all
```

Registre a origem e o destino entre clusters LIFs

SnapMirror usa interfaces lógicas entre clusters (LIFs), cada uma com um endereço IP exclusivo, para facilitar a transferência de dados entre os clusters de origem e de destino.

1. Para o destino FSx dos sistemas de arquivos ONTAP, você pode recuperar o endpoint entre clusters - endereços IP do FSx console da Amazon navegando até a guia Administração na página de detalhes do seu sistema de arquivos.
2. Para o cluster NetApp ONTAP de origem, recupere os endereços IP LIF entre clusters usando a CLI ONTAP. Execute o seguinte comando:

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

> **Note**
>
> Para sistemas de arquivos Single-AZ de segunda geração, há dois endereços IP entre clusters para cada par de alta disponibilidade (HA). Salve esses valores para uso posterior.

Salve os endereços IP `inter_1` e `inter_2`. Eles são referidos no `FSx-Dest` como `dest_inter_1` e `dest_inter_2` e em `OnPrem-Source` como `source_inter_1` e `source_inter_2`.

Estabelecer o emparelhamento de clusters entre a origem e o destino

Estabeleça um relacionamento entre pares de clusters no cluster de destino fornecendo os endereços IP entre clusters. Você também precisará criar uma senha que deverá ser inserida ao estabelecer o emparelhamento de clusters no cluster de origem.

1. Defina o emparelhamento no cluster de destino usando o seguinte comando. Para sistemas de arquivos Single-AZ de segunda geração, você precisará fornecer cada endereço IP entre clusters.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. Em seguida, estabeleça o relacionamento entre pares do cluster no cluster de origem. Você precisará digitar a senha criada acima para se autenticar. Para sistemas de arquivos Single-AZ de segunda geração, você precisará fornecer cada endereço IP entre clusters.

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. Verifique se o emparelhamento foi bem-sucedido usando o comando a seguir no cluster de origem. Na saída, `Availability` deve ser definida como `Available`.

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
```

```
FSx-Dest            Available      ok
```

Criar um relacionamento de emparelhamento entre SVMs

Com o peering de cluster estabelecido, a próxima etapa é emparelhar o. SVMs Crie um relacionamento de emparelhamento de SVM no cluster de destino (FSx-Dest) usando o comando. `vserver peer` Estes são os aliases adicionais usados nos comandos a seguir.

- `DestLocalName`: esse é o nome usado para identificar a SVM de destino ao configurar o emparelhamento entre SVMs na SVM de origem.
- `SourceLocalName`: esse é o nome usado para identificar a SVM de origem ao configurar o emparelhamento entre SVMs na SVM de destino.

1. Use o comando a seguir para criar uma relação de emparelhamento de SVM entre a origem e o destino. SVMs

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName

 Info: [Job 207] 'vserver peer create' job queued
```

2. Aceite o relacionamento de emparelhamento no cluster de origem:

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. Verifique o status de emparelhamento da SVM usando o comando a seguir; `Peer State` deve ser definido como `peered` na resposta.

```
OnPrem-Source::> vserver peer show

        Peer     Peer   Peer     Peering       Remote
Vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------- ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

Crie o SnapMirror relacionamento

Agora que você emparelhou a origem e o destino SVMs, as próximas etapas são criar e inicializar o SnapMirror relacionamento no cluster de destino.

> **Note**
>
> Depois de criar e inicializar um SnapMirror relacionamento, os volumes de destino ficam somente para leitura até que o relacionamento seja interrompido.

- Use o `snapmirror create` comando para criar o SnapMirror relacionamento no cluster de destino. O comando `snapmirror create` deve ser usado na SVM de destino.

  Opcionalmente, você pode usar `-throttle` para definir a largura de banda máxima (em KB/s) para o relacionamento. SnapMirror

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
path DestSVM:vol1 -vserver DestSVM -throttle unlimited

 Operation succeeded: snapmirror create for the relationship with destination
 "DestSVM:vol1".
```

Transfira dados para o seu sistema FSx de arquivos para ONTAP

Agora que você criou o SnapMirror relacionamento, você pode transferir dados para o sistema de arquivos de destino.

1. Você pode transferir dados para o sistema de arquivos de destino executando o comando a seguir no sistema de arquivos de destino.

   > **Note**
   >
   > Depois de executar esse comando, SnapMirror começa a transferir instantâneos de dados do volume de origem para o volume de destino.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
path SourceLocalName:vol1
```

2. Se estiver migrando dados que estão sendo usados ativamente, precisará atualizar seu cluster de destino para que permaneça sincronizado com o cluster de origem. Para executar uma atualização única no cluster de destino, execute o comando a seguir.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

3. Você também pode agendar atualizações de hora em hora ou diárias antes de concluir a migração e transferir seus clientes FSx para o ONTAP. Você pode estabelecer um cronograma de SnapMirror atualização usando o `snapmirror modify`comando.

```
FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
```

Passando para a Amazon FSx

Para se preparar para a transferência FSx para seu sistema de arquivos do ONTAP, faça o seguinte:

- Desconecte todos os clientes que gravam no cluster de origem.
- Execute uma SnapMirror transferência final para garantir que não haja perda de dados durante o recorte.
- Rompa o SnapMirror relacionamento.
- Conecte todos os clientes ao seu sistema de arquivos FSx for ONTAP.

1. Para garantir que todos os dados do cluster de origem sejam transferidos FSx para o sistema de arquivos ONTAP, execute uma transferência final do Snapmirror.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. Certifique-se de que a migração dos dados esteja concluída verificando se o `Mirror State` está definido como `Snapmirrored` e se o `Relationship Status` está definido como `Idle`. Você também deve garantir que a data de `Last Transfer End Timestamp` seja a esperada, pois mostra quando ocorreu a última transferência para o volume de destino.
3. Execute o comando a seguir para mostrar o SnapMirror status.

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      --------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. Desative quaisquer SnapMirror transferências futuras usando o `snapmirror quiesce` comando.

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. Verifique se o `Relationship Status` mudou para `Quiesced` usando `snapmirror show`.

```
FSx-Dest::> snapmirror show

Source           Destination   Mirror        Relationship
Path             Path          State         Status
-----------      ------------  ------------- --------
sourcesvm1:vol1  svm01:DestVol Snapmirrored  Quiesced
```

6. Durante a migração, o volume de destino é somente leitura. Para habilitar a leitura/gravação, você precisa romper o SnapMirror relacionamento e passar para o sistema de arquivos do FSx ONTAP. Quebre o SnapMirror relacionamento usando o comando a seguir.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. Depois que a SnapMirror replicação for concluída e você romper o SnapMirror relacionamento, você poderá montar o volume para disponibilizar os dados.

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

O volume já está disponível com os dados do volume de origem totalmente migrados para o volume de destino. O volume também está disponível para os clientes lerem e gravarem nele. Se você definiu anteriormente a `tiering-policy` desse volume como `all`, poderá alterá-la para `auto` ou `snapshot-only` e seus dados farão a transição automática entre os níveis de armazenamento

de acordo com os padrões de acesso. Para tornar esses dados acessíveis a clientes e aplicações, consulte Acessando seus dados FSx do ONTAP.

Migrando FSx para o ONTAP usando AWS DataSync

Recomendamos usar AWS DataSync para transferir dados entre FSx sistemas de arquivos ONTAP e sistemas de arquivos não ONTAP, inclusive FSx para Lustre, para OpenZFS, FSx para FSx Windows File Server, Amazon EFS, Amazon S3 e arquivadores locais. Se você estiver transferindo arquivos entre FSx o ONTAP e o NetApp ONTAP, recomendamos usar. NetApp SnapMirror AWS DataSync é um serviço de transferência de dados que simplifica, automatiza e acelera a movimentação e a replicação de dados entre sistemas de armazenamento autogerenciados e serviços de armazenamento pela AWS Internet ou. AWS Direct Connect DataSync pode transferir dados e metadados do sistema de arquivos, como propriedade, registros de data e hora e permissões de acesso.

Você pode usar DataSync para transferir arquivos entre dois FSx para sistemas de arquivos ONTAP e também mover dados para um sistema de arquivos em uma AWS conta Região da AWS ou diferente. Você também pode usar DataSync com sistemas FSx de arquivos ONTAP para outras tarefas. Por exemplo, você pode executar migrações de dados únicas, ingerir dados periodicamente para workloads distribuídas e programar a replicação para proteção e recuperação de dados.

Em DataSync, um local é um endpoint para um sistema de arquivos FSx para ONTAP. Para obter informações sobre cenários de transferência específicos, consulte Working with locations no Guia do usuário do AWS DataSync .

> **Note**
>
> Se você planeja usar a política de divisão em níveis `All` para migrar seus dados para o nível do grupo de capacidade, tenha em mente que os metadados do arquivo são sempre armazenados no nível SSD e que todos os novos dados do usuário são gravados primeiro no nível SSD. Quando os dados são gravados no nível SSD, o processo de divisão em níveis em segundo plano começa a dividir seus dados no armazenamento do grupo de capacidade, mas esse processo não é imediato e consome recursos da rede. É necessário dimensionar seu nível SSD para contabilizar os metadados do arquivo (de 3 a 7% do tamanho dos dados do usuário), como um buffer para os dados do usuário, antes de serem divididos em níveis no armazenamento do grupo de capacidade. Recomendamos que não exceda 80% de utilização do SSD.

Ao migrar dados, monitore sua camada de SSD usando métricas do sistema de CloudWatch arquivos para garantir que ela não seja preenchida mais rápido do que o processo de hierarquização pode mover os dados para o armazenamento do pool de capacidade. Você também pode reduzir as DataSync transferências para uma taxa menor do que a taxa em que a hierarquização está ocorrendo para garantir que seu nível de SSD não exceda 80% de utilização. Por exemplo, para sistemas de arquivos com uma capacidade de taxa de transferência de pelo menos 512 MBps, um MBps acelerador de 200 normalmente equilibra as taxas de transferência de dados e de armazenamento de dados em camadas.

Pré-requisitos

Para migrar dados FSx para sua configuração do ONTAP, você precisa de um servidor e uma rede que atendam aos DataSync requisitos. Para saber mais, consulte os requisitos DataSync do Guia AWS DataSync do usuário.

Etapas básicas para migrar arquivos usando DataSync

A transferência de arquivos de uma origem para um destino usando DataSync envolve as seguintes etapas básicas:

- Baixe e implante um agente em seu ambiente e ative-o (não é necessário se estiver transferindo entre eles Serviços da AWS).
- Crie um local de origem e de destino.
- Crie uma tarefa do .
- Execute a tarefa para transferir arquivos da origem para o destino.

Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS DataSync :

- Transferência de dados entre armazenamento autogerenciado e AWS
- Criação de um local para a Amazon FSx para NetApp ONTAP

Segurança na Amazon FSx para NetApp ONTAP

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam à Amazon FSx para o NetApp ONTAP, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar a Amazon FSx. Os tópicos a seguir mostram como configurar a Amazon FSx para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam você a monitorar e proteger seus FSx recursos da Amazon.

Tópicos

- Proteção de dados na Amazon FSx para NetApp ONTAP
- Gerenciamento de identidade e acesso da Amazon FSx para NetApp ONTAP
- AWS políticas gerenciadas para Amazon FSx for OpenZFS
- Controle de acesso ao sistema de arquivos com a Amazon VPC
- Validação de conformidade da Amazon FSx para NetApp ONTAP
- Amazon FSx para NetApp ONTAP e endpoints VPC de interface ()AWS PrivateLink
- Resiliência na Amazon FSx para ONTAP NetApp
- Segurança de infraestrutura na Amazon FSx para NetApp ONTAP
- Use o NetApp ONTAP Vscan com FSx o ONTAP

- Usuários e perfis do ONTAP

Proteção de dados na Amazon FSx para NetApp ONTAP

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados na Amazon FSx para NetApp ONTAP. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso

inclui quando você trabalha com a Amazon FSx ou outra Serviços da AWS pessoa usando o console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Criptografia de dados FSx para ONTAP

O Amazon FSx for NetApp ONTAP oferece suporte à criptografia de dados em repouso e à criptografia de dados em trânsito. A criptografia de dados em repouso é ativada automaticamente ao criar um sistema de FSx arquivos da Amazon. O Amazon FSx for NetApp ONTAP oferece suporte à criptografia baseada em Kerberos em trânsito pelos protocolos NFS e SMB se você estiver acessando dados em uma Máquina Virtual de Armazenamento (SVM) associada a um Active Directory ou a um domínio usando o Lightweight Directory Access Protocol (LDAP).

Quando usar a criptografia

Se sua organização estiver sujeita a políticas corporativas ou regulatórias que exigem criptografia de dados e metadados em repouso, seus dados serão automaticamente criptografados em repouso. É recomendável também que você habilite a criptografia de dados em trânsito montando seu sistema de arquivos com o uso da criptografia de dados em trânsito.

Para obter mais informações sobre criptografia de dados com a Amazon FSx for NetApp ONTAP, consulte Criptografia de dados em repouso e. Criptografia de dados em trânsito

Criptografia de dados em repouso

Todos os sistemas de arquivos e backups do Amazon FSx for NetApp ONTAP são criptografados em repouso com chaves gerenciadas usando AWS Key Management Service (AWS KMS). Os dados são criptografados automaticamente antes de serem gravados no sistema de arquivos e automaticamente decriptografados à medida que são lidos. Todos os backups são criptografados automaticamente na criação e descriptografados automaticamente quando o backup é restaurado em um novo volume. Esses processos são gerenciados de forma transparente pela Amazon FSx, para que você não precise modificar seus aplicativos.

A Amazon FSx usa um algoritmo de criptografia AES-256 padrão do setor para criptografar dados e metadados da Amazon FSx em repouso. Para obter mais informações, consulte Conceitos básicos de criptografia no Guia do desenvolvedor do AWS Key Management Service .

> **Note**
>
> A infraestrutura de gerenciamento de AWS chaves usa algoritmos criptográficos aprovados pelo Federal Information Processing Standards (FIPS) 140-2. A infraestrutura é consistente com as recomendações 800-57 do National Institute of Standards and Technology (NIST).

Como a Amazon FSx usa AWS KMS

A Amazon FSx se integra ao gerenciamento AWS KMS de chaves. A Amazon FSx usa chaves KMS para criptografar seu sistema de arquivos e qualquer backup de volume. Você escolhe a chave KMS usada para criptografar e descriptografar sistemas de arquivos e backups de volume (dados e metadados). É possível habilitar, desabilitar ou revogar as concessões nessa chave do KMS. Essa chave do KMS pode ser de um dos seguintes dois tipos:

- chave KMS gerenciada pela AWS: essa é a chave KMS padrão e de uso gratuito.
- chave KMS gerenciada pelo cliente: essa é a chave KMS mais flexível em termos de uso, pois é possível configurar suas políticas de chaves e concessões para vários usuários ou serviços. Para obter mais informações sobre a criação de chaves KMS, consulte Criação de chaves no Guia do AWS Key Management Service desenvolvedor.

> **Important**
>
> A Amazon FSx aceita somente chaves KMS de criptografia simétrica. Você não pode usar chaves KMS assimétricas com a Amazon. FSx

Se você usa uma chave KMS gerenciada pelo cliente como sua chave KMS de criptografia e decriptografia de dados de arquivos, pode habilitar a rotação de chaves. Ao habilitar a rotação de chaves, o AWS KMS gira sua chave automaticamente uma vez por ano. Além disso, com uma chave KMS gerenciada pelo cliente, você pode escolher quando desabilitar, reabilitar, excluir ou revogar o acesso à sua KMS a qualquer momento. Para obter mais informações, consulte Rotação de AWS KMS keys e Como ativar e desativar chaves no Guia do desenvolvedor do AWS Key Management Service .

FSx Políticas-chave da Amazon para AWS KMS

Políticas de chaves são a principal maneira de controlar o acesso a chaves do KMS. Para obter mais informações sobre as políticas de chaves, consulte Using key policies in AWS KMS no Guia do desenvolvedor do AWS Key Management Service .A lista a seguir descreve todas as permissões AWS KMS relacionadas suportadas pela Amazon FSx para sistemas de arquivos e backups criptografados em repouso:

- kms:Encrypt - (Opcional) Criptografa texto simples em texto cifrado. Essa permissão está incluída na política de chaves padrão.
- kms:Decrypt: (obrigatório) descriptografa texto cifrado. O texto cifrado é o texto simples que já foi criptografado. Essa permissão está incluída na política de chaves padrão.
- kms: ReEncrypt — (Opcional) Criptografa os dados no lado do servidor com um novo AWS KMS key, sem expor o texto simples dos dados no lado do cliente. Primeiro os dados são descriptografados e, depois, recriptografados. Essa permissão está incluída na política de chaves padrão.
- kms: GenerateDataKeyWithoutPlaintext — (Obrigatório) Retorna uma chave de criptografia de dados criptografada sob uma chave KMS. Essa permissão está incluída na política de chaves padrão em kms: GenerateDataKey *.
- kms: CreateGrant — (Obrigatório) Adiciona uma concessão a uma chave para especificar quem pode usar a chave e sob quais condições. Concessões são mecanismos de permissão alternativos para políticas de chaves. Para obter mais informações sobre concessões, consulte Usar concessões no Guia do desenvolvedor do AWS Key Management Service . Essa permissão está incluída na política de chaves padrão.
- kms: DescribeKey — (Obrigatório) Fornece informações detalhadas sobre a chave KMS especificada. Essa permissão está incluída na política de chaves padrão.
- kms: ListAliases — (Opcional) Lista todos os aliases de chave na conta. Quando você usa o console para criar um sistema de arquivos criptografado, essa permissão preenche a lista de chaves do KMS. Recomendamos usar essa permissão para proporcionar a melhor experiência do usuário. Essa permissão está incluída na política de chaves padrão.

Criptografia de dados em trânsito

Este tópico explica as diferentes opções disponíveis para criptografar os dados do arquivo enquanto eles estão em trânsito entre um FSx sistema de arquivos do ONTAP e os clientes conectados.

Ele também oferece orientação para ajudar você a escolher qual o método de criptografia mais adequado para seu fluxo de trabalho.

Todos os dados que fluem Regiões da AWS pela rede AWS global são criptografados automaticamente na camada física antes de saírem das instalações AWS protegidas. Todo o tráfego entre as zonas de disponibilidade é criptografado. Camadas adicionais de criptografia, inclusive as listadas nesta seção, fornecem mais proteções. Para obter mais informações sobre como AWS fornece proteção para o fluxo de dados Regiões da AWS, zonas disponíveis e instâncias, consulte Criptografia em trânsito no Guia do usuário do Amazon Elastic Compute Cloud para instâncias Linux.

O Amazon FSx for NetApp ONTAP oferece suporte aos seguintes métodos para criptografar dados em trânsito entre FSx os sistemas de arquivos ONTAP e os clientes conectados:

- Criptografia automática baseada em Nitro em todos os protocolos e clientes compatíveis em execução nos tipos de instância Amazon EC2 Linux e Windows compatíveis.
- Criptografia baseada em Kerberos com os protocolos NFS e SMB.
- IPseccriptografia baseada em protocolos NFS, iSCSI e SMB

Todos os métodos suportados para criptografar dados em trânsito usam algoritmos criptográficos AES-256 padrão do setor que fornecem criptografia de força corporativa.

Tópicos

- Como escolher um método para criptografar dados em trânsito
- Criptografando dados em trânsito com o AWS Nitro System
- Criptografia de dados em trânsito com criptografia baseada em Kerberos
- Criptografando dados em trânsito com IPsec criptografia
- Habilitar a criptografia de SMB para dados em trânsito
- Configurando IPsec usando a autenticação PSK
- Configurando IPsec usando a autenticação de certificado

Como escolher um método para criptografar dados em trânsito

Esta seção fornece informações que podem ajudar você a decidir qual dos métodos de criptografia em trânsito com suporte é melhor para seu fluxo de trabalho. Consulte esta seção novamente ao explorar as opções com suporte descritas detalhadamente nas seções a seguir.

Há vários fatores a serem considerados ao escolher como você criptografará os dados em trânsito entre o sistema de arquivos FSx for ONTAP e os clientes conectados. Esses fatores incluem:

- O em Região da AWS que seu sistema de arquivos FSx for ONTAP está sendo executado.
- O tipo de instância no qual o cliente está sendo executado.
- A localização do cliente que está acessando o sistema de arquivos.
- Requisitos de performance da rede.
- O protocolo de dados que você deseja criptografar.
- Se estiver usando o Microsoft Active Directory.

Região da AWS

A configuração em Região da AWS que seu sistema de arquivos está sendo executado determina se você pode ou não usar a criptografia baseada no Amazon Nitro. Para obter mais informações, consulte Criptografando dados em trânsito com o AWS Nitro System.

Tipo de instância do cliente

Você pode usar a criptografia baseada no Amazon Nitro se o cliente que está acessando seu sistema de arquivos estiver sendo executado em qualquer um dos tipos de instância Amazon EC2 Mac, Linux ou Windows compatíveis, e seu fluxo de trabalho atender a todos os outros requisitos de uso da criptografia baseada em Nitro. Não há requisitos de tipo de instância de cliente para usar o Kerberos ou IPsec a criptografia.

Client location (Localização do cliente)

A localização do cliente que acessa dados em relação à localização do sistema de arquivos afeta quais métodos de criptografia em trânsito estão disponíveis para uso. Você poderá usar qualquer um dos métodos de criptografia com suporte se o cliente e o sistema de arquivos estiverem localizados na mesma VPC. O mesmo acontece se o cliente e o sistema de arquivos estiverem localizados em peering VPCs, desde que o tráfego não passe por um dispositivo ou serviço de rede virtual, como um gateway de trânsito. A criptografia baseada em Nitro não será uma opção disponível se o cliente não estiver na mesma VPC ou na VPC emparelhada, ou se o tráfego passar por um dispositivo ou serviço de rede virtual.

Performance de rede

O uso da criptografia baseada no Amazon Nitro não tem impacto na performance da rede. Isso ocorre porque as EC2 instâncias suportadas da Amazon utilizam os recursos de descarga do

hardware subjacente do Nitro System para criptografar automaticamente o tráfego em trânsito entre as instâncias.

O uso do Kerberos ou da IPsec criptografia tem um impacto no desempenho da rede. Isso ocorre porque esses dois métodos de criptografia são baseados em software, o que exige que o cliente e o servidor usem recursos de computação para criptografar e decriptografar o tráfego em trânsito.

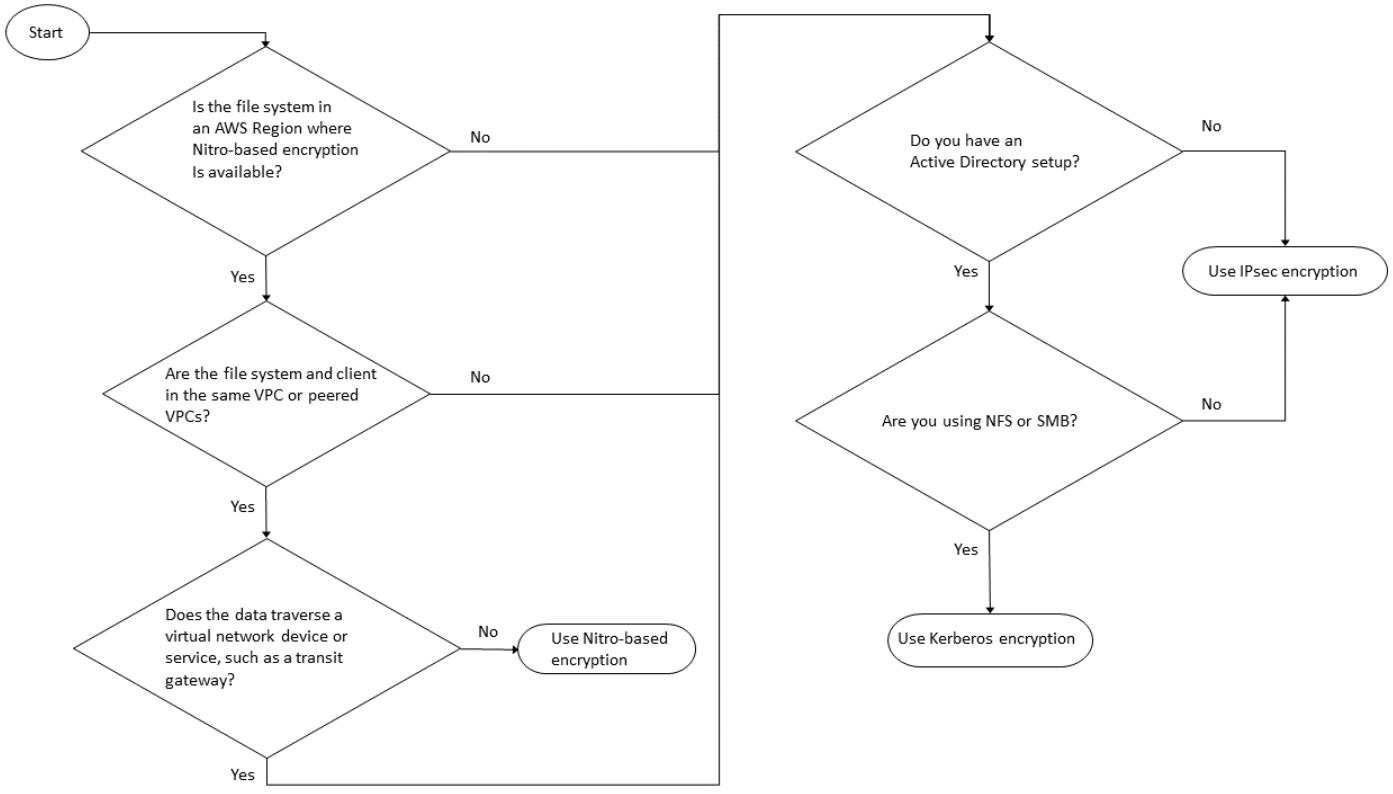
Protocolo de dados

Você pode usar criptografia e IPsec criptografia baseadas no Amazon Nitro com todos os protocolos compatíveis — NFS, SMB e iSCSI. Você pode usar a criptografia Kerberos com os protocolos NFS e SMB (com um Active Directory).

Active Directory

Se você estiver usando o Microsoft Active Directory, poderá usar a criptografia Kerberos nos protocolos NFS e SMB.

Use o diagrama a seguir como ajuda para decidir qual método de criptografia em trânsito usar.



IPsec a criptografia é a única opção disponível quando todas as condições a seguir se aplicam ao seu fluxo de trabalho:

- Você está usando o protocolo NFS, SMB ou iSCSI.
- Seu fluxo de trabalho não dá suporte ao uso da criptografia baseada no Amazon Nitro.
- Você não está usando um domínio do Microsoft Active Directory.

Criptografando dados em trânsito com o AWS Nitro System

Com a criptografia baseada em Nitro, os dados em trânsito são criptografados automaticamente quando os clientes que acessam seus sistemas de arquivos estão executando em tipos de instância Amazon EC2 Linux ou Windows compatíveis, Regiões da AWS onde estão disponíveis no FSx ONTAP.

O uso da criptografia baseada no Amazon Nitro não tem impacto na performance da rede. Isso ocorre porque as EC2 instâncias suportadas da Amazon utilizam os recursos de descarga do hardware subjacente do Nitro System para criptografar automaticamente o tráfego em trânsito entre as instâncias.

A criptografia baseada em Nitro é habilitada automaticamente quando os tipos de instância de cliente com suporte estão localizados na mesma Região da AWS e na mesma VPC ou em uma VPC emparelhada com a VPC do sistema de arquivos. Além disso, se o cliente estiver em uma VPC emparelhada, os dados não poderão passar por um dispositivo ou serviço de rede virtual (como um gateway de trânsito) para que a criptografia baseada em Nitro seja habilitada automaticamente. Para obter mais informações sobre criptografia baseada em Nitro, consulte a seção Criptografia em trânsito do Guia EC2 do usuário da Amazon para tipos de instância Linux ou Windows.

A tabela a seguir detalha em Regiões da AWS que a criptografia baseada em Nitro está disponível.

Compatibilidade com criptografia baseada em Nitro

Geração	Tipos de implantação	Região da AWS
Sistemas de arquivos de primeira geração[1]	Single-AZ 1 Multi-AZ 1	Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon), Europa (Irlanda)

Geração	Tipos de implantação	Região da AWS
Sistemas de arquivos de segunda geração	Single-AZ 2 Multi-AZ 2	Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Norte da Califórnia), Oeste dos EUA (Oregon), Europa (Frankfurt), Europa (Irlanda), Ásia-Pacífico (Sydney)

[1] Os sistemas de arquivos de primeira geração criados a partir de 28 de novembro de 2022 são compatíveis com criptografia em trânsito baseada em Nitro nas Regiões da AWS listadas.

Para obter mais informações sobre Regiões da AWS onde FSx o ONTAP está disponível, consulte Amazon FSx for NetApp ONTAP Pricing.

Para obter mais informações sobre as especificações de desempenho dos sistemas de FSx arquivos ONTAP, consulteImpacto da capacidade de throughput na performance.

Criptografia de dados em trânsito com criptografia baseada em Kerberos

Se você estiver usando o Microsoft Active Directory, poderá usar a criptografia baseada em Kerberos nos protocolos NFS e SMB para criptografar dados em trânsito para volumes secundários associados a um Microsoft Active Directory. SVMs

Criptografia de dados em trânsito pelo NFS usando Kerberos

A criptografia de dados em trânsito usando Kerberos tem suporte e protocolos NFSv3 . NFSv4 Para habilitar a criptografia em trânsito usando o Kerberos com o protocolo NFS, consulte Uso do Kerberos com NFS para segurança forte no Centro de documentação do NetApp ONTAP

Criptografia de dados em trânsito pelo SMB usando Kerberos

Há suporte para criptografia de dados em trânsito pelo protocolo SMB nos compartilhamentos de arquivos mapeados em uma instância de computação compatível com o protocolo SMB 3.0 ou mais recente. Isso inclui todas as versões do Microsoft Windows do Microsoft Windows Server 2012 e posterior e do Microsoft Windows 8 e posterior. Quando ativado, o FSx for ONTAP criptografa automaticamente os dados em trânsito usando a criptografia SMB à medida que você acessa seu sistema de arquivos sem a necessidade de modificar seus aplicativos.

FSx para ONTAP, o SMB suporta criptografia de 128 e 256 bits, que é determinada pela solicitação da sessão do cliente. Para obter descrições dos diferentes níveis de criptografia, consulte a seção Definir o nível mínimo de segurança de autenticação do servidor SMB em Gerenciar SMB com a CLI no Centro de documentação do NetApp ONTAP.

> **Note**
>
> O cliente determina o algoritmo de criptografia. As autenticações NTLM e Kerberos funcionam com criptografia de 128 e 256 bits. O FSx for ONTAP SMB Server aceita todas as solicitações padrão do cliente Windows, e os controles granulares são gerenciados pelas configurações da Política de Grupo ou do Registro da Microsoft.

Você usa a ONTAP CLI para gerenciar as configurações de criptografia em trânsito FSx para ONTAP SVMs e volumes. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na SVM na qual você está definindo as configurações de criptografia em trânsito, conforme descrito em Gerenciando SVMs com o ONTAP CLI.

Para obter informações sobre como habilitar a criptografia de SMB em uma SVM ou volume, consulte Habilitar a criptografia de SMB para dados em trânsito.

Criptografando dados em trânsito com IPsec criptografia

FSx for ONTAP suporta o uso do IPsec protocolo no modo de transporte para garantir que os dados estejam continuamente seguros e criptografados enquanto estão em trânsito. IPsec oferece end-to-end criptografia de dados em trânsito entre clientes e FSx para sistemas de arquivos ONTAP para todo o tráfego IP suportado — protocolos NFS, iSCSI e SMB. Com a IPsec criptografia, você estabelece um IPsec túnel entre um FSx para ONTAP SVM configurado com IPsec ativado e um IPsec cliente em execução no cliente conectado acessando os dados.

Recomendamos que você use IPsec para criptografar dados em trânsito pelos protocolos NFS, SMB e iSCSI ao acessar seus dados de clientes que não oferecem suporte à criptografia baseada em Nitro e se seu cliente não SVMs estiverem associados a um Active Directory, o que é necessário para criptografia baseada em Kerberos. IPsec a criptografia é a única opção disponível para criptografar dados em trânsito para tráfego iSCSI quando seu cliente iSCSI não oferece suporte à criptografia baseada em Nitro.

Para IPsec autenticação, você pode usar chaves pré-compartilhadas (PSKs) ou certificados. Se você estiver usando uma PSK, o IPsec cliente que você usa deve oferecer suporte ao Internet

Key Exchange versão 2 (IKEv2) com uma PSK. As etapas de alto nível para configurar a IPsec criptografia no ONTAP e no cliente são as seguintes: FSx

1. Ative e configure IPsec em seu sistema de arquivos.
2. Instale e configure IPsec em seu cliente
3. Configurar IPsec para acesso a vários clientes

Para obter mais informações sobre como configurar IPsec usando PSK, consulte Configurar a segurança IP (IPsec) por meio de criptografia com fio no centro de NetApp ONTAP documentação.

Para obter mais informações sobre como configurar IPsec usando certificados, consulteConfigurando IPsec usando a autenticação de certificado.

Habilitar a criptografia de SMB para dados em trânsito

Por padrão, quando você cria uma SVM, a criptografia SMB é desativada. Você pode habilitar a criptografia SMB necessária em compartilhamentos individuais ou em uma SVM, o que a ativa para todos os compartilhamentos nessa SVM.

> **Note**
>
> Quando a criptografia SMB necessária está habilitada em uma SVM ou em um compartilhamento, os clientes SMB que não oferecem suporte à criptografia não podem se conectar à SVM ou ao compartilhamento.

Para exigir criptografia SMB no tráfego SMB de entrada em uma SVM

Use o procedimento a seguir para exigir criptografia SMB em uma SVM usando a CLI do NetApp ONTAP.

1. Para se conectar ao endpoint de gerenciamento da SVM com SSH, use o nome de usuário `vsadmin` e a senha vsadmin definidos ao criar a SVM. Se você não tiver definido uma senha vsadmin, utilize o nome de usuário `fsxadmin` e a senha fsxadmin. Você pode efetuar SSH na SVM por meio de um cliente que esteja na mesma VPC do sistema de arquivos, usando o endereço IP ou o nome DNS do endpoint de gerenciamento.

   ```
   ssh vsadmin@svm-management-endpoint-ip-address
   ```

O comando com exemplo de valores:

```
ssh vsadmin@198.51.100.10
```

O comando SSH usando o nome DNS do endpoint de gerenciamento:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

O comando de SSH usando um nome de DNS de exemplo:

```
ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-
east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxIdabcdef01234567892::>
```

2. Use o comando `vserver cifs security modify` da CLI do NetApp ONTAP para exigir criptografia de SMB para o tráfego SMB recebido na SVM.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
```

3. Para deixar de exigir a criptografia SMB no tráfego SMB de entrada, use o comando a seguir.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required
 false
```

4. Para ver a configuração `is-smb-encryption-required` atual em uma SVM, use o seguinte comando `vserver cifs security show` da CLI do NetApp ONTAP:

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-------- ------------------------
vs1      true
```

Para obter mais informações sobre como gerenciar a criptografia SMB em uma SVM, consulte Configuração da criptografia SMB necessária em servidores SMB para transferências de dados por SMB no Centro de documentação do NetApp ONTAP,

Habilitar a criptografia SMB em um volume

Use o procedimento a seguir para exigir criptografia SMB em um compartilhamento usando a CLI do NetApp ONTAP.

1. Estabeleça uma conexão Secure Shell (SSH) com o endpoint de gerenciamento da SVM, conforme descrito em Gerenciando SVMs com o ONTAP CLI.
2. Use o comando da CLI do NetApp ONTAP a seguir para criar um novo compartilhamento SMB e exigir criptografia SMB ao acessar esse compartilhamento.

   ```
   vserver cifs share create -vserver vserver_name -share-name share_name -
   path share_path -share-properties encrypt-data
   ```

   Para obter mais informações, consulte `vserver cifs share create` nas páginas de manual de comandos da CLI do NetApp ONTAP.
3. Para exigir a criptografia SMB em um compartilhamento SMB existente, use o comando a seguir.

   ```
   vserver cifs share properties add -vserver vserver_name -share-name share_name -
   share-properties encrypt-data
   ```

   Para obter mais informações, consulte `vserver cifs share create` nas páginas de manual de comandos da CLI do NetApp ONTAP.
4. Para desativar a criptografia SMB em um compartilhamento SMB existente, use o comando a seguir.

   ```
   vserver cifs share properties remove -vserver vserver_name -share-name share_name -
   share-properties encrypt-data
   ```

   Para obter mais informações, consulte `vserver cifs share properties remove` nas páginas de manual de comandos da CLI do NetApp ONTAP.
5. Para ver a configuração atual `is-smb-encryption-required` em um compartilhamento SMB, use o seguinte comando da CLI do NetApp ONTAP:

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -
fields share-properties
```

Se uma das propriedades retornadas pelo comando for `encrypt-data`, essa propriedade especificará que a criptografia SMB deve ser usada ao acessar esse compartilhamento.

Para obter mais informações, consulte `vserver cifs share properties show` nas páginas de manual de comandos da CLI do NetApp ONTAP.

Configurando IPsec usando a autenticação PSK

Se você estiver usando o PSK para autenticação, as etapas para configurar a IPsec criptografia no ONTAP e no cliente são as seguintes: FSx

1. Ative e configure IPsec em seu sistema de arquivos.
2. Instale e configure IPsec em seu cliente
3. Configurar IPsec para acesso a vários clientes

Para obter detalhes sobre a configuração IPsec usando o PSK, consulte Configurar a segurança IP (IPsec) por criptografia eletrônica no centro de NetApp ONTAP documentação.

Configurando IPsec usando a autenticação de certificado

Os tópicos a seguir fornecem instruções para configurar a IPsec criptografia usando a autenticação de certificado em um sistema de arquivos FSx for ONTAP e em um cliente executando o Libreswan. IPsec Essa solução usa AWS Certificate Manager e AWS Private Certificate Authority para criar uma autoridade de certificação privada e para gerar os certificados.

As etapas de alto nível para configurar a IPsec criptografia usando a autenticação de certificado em sistemas FSx de arquivos ONTAP e clientes conectados são as seguintes:

1. Ter uma autoridade de certificação implantada para emitir certificados.
2. Gerar e exportar certificados de CA para o sistema de arquivos e o cliente.
3. Instale o certificado e configure IPsec na instância do cliente.
4. Instale o certificado e configure IPsec em seu sistema de arquivos.
5. Definir o banco de dados de políticas de segurança (SPD).

6. Configure IPsec para acesso a vários clientes.

Como criar e instalar certificados CA

Para autenticação de certificados, você precisa gerar e instalar certificados de uma autoridade de certificação em seu sistema FSx de arquivos do ONTAP e dos clientes que acessarão os dados em seu sistema de arquivos. O exemplo a seguir é usado AWS Private Certificate Authority para configurar uma autoridade de certificação privada e gerar os certificados para instalação no sistema de arquivos e no cliente. Usando AWS Private Certificate Authority, você pode criar uma hierarquia totalmente AWS hospedada de autoridades de certificação raiz e subordinadas (CAs) para uso interno de sua organização. Esse processo tem cinco etapas:

1. Crie uma autoridade de certificação (CA) privada usando AWS Private CA
2. Emitir e instalar o certificado raiz na CA privada
3. Solicite um certificado privado AWS Certificate Manager para seu sistema de arquivos e clientes
4. Exportar o certificado para o sistema de arquivos e os clientes

Para obter mais informações, consulte Administração de CA privada no Guia AWS Private Certificate Authority do usuário.

Criar a CA privada raiz

1. Ao criar uma CA, especifique a configuração da CA em um arquivo fornecido por você. O comando a seguir usa o editor de texto Nano para criar o arquivo `ca_config.txt`, que especifica as seguintes informações:

   - O nome do algoritmo
   - O algoritmo de assinatura que a CA usa para assinar
   - Informações do assunto X.500

   ```
   $ > nano ca_config.txt
   ```

   O editor de texto é exibido.
2. Edite o arquivo com as especificações da sua CA.

   ```
   {
   ```

```
   "KeyAlgorithm":"RSA_2048",
   "SigningAlgorithm":"SHA256WITHRSA",
   "Subject":{
      "Country":"US",
      "Organization":"Example Corp",
      "OrganizationalUnit":"Sales",
      "State":"WA",
      "Locality":"Seattle",
      "CommonName":"*.ec2.internal"
   }
}
```

3. Salve e feche o arquivo, saindo do editor de texto. Para obter mais informações, consulte Procedimento para criar uma CA no Guia AWS Private Certificate Authority do Usuário.
4. Use o comando create-certificate-authority AWS Private CA CLI para criar uma CA privada.

```
~/home > aws acm-pca create-certificate-authority \
     --certificate-authority-configuration file://ca_config.txt \
     --certificate-authority-type "ROOT" \
     --idempotency-token 01234567 --region aws-region
```

Se obtiver êxito, esse comando produz o nome de recurso da Amazon (ARN) da CA.

```
{
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Para criar e instalar um certificado para a CA raiz privada (AWS CLI)

1. Gere uma solicitação de assinatura de certificado (CSR) usando o comando get-certificate-authority-csr AWS CLI.

```
$ aws acm-pca get-certificate-authority-csr \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --output text \
     --endpoint https://acm-pca.aws-region.amazonaws.com \
     --region eu-west-1 > ca.csr
```

O arquivo resultante `ca.csr`, um arquivo PEM codificado no formato base64, tem a seguinte aparência.

```
-----BEGIN CERTIFICATE-----
 MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
 VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
 BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
 MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
 VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
 b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
 YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
 rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
 Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
 FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
 NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
 -----END CERTIFICATE-----
```

Para obter mais informações, consulte Instalando um certificado CA raiz no Guia AWS Private Certificate Authority do usuário.

2. Use o `issue-certificate` AWS CLI comando para emitir e instalar o certificado raiz em sua CA privada.

```
$ aws acm-pca issue-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --csr file://ca.csr \
     --signing-algorithm SHA256WITHRSA \
     --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
     --validity Value=3650,Type=DAYS --region aws-region
```

3. Faça o download do certificado raiz usando o `get-certificate` AWS CLI comando.

```
$ aws acm-pca get-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
```

```
    --output text --region aws-region > rootCA.pem
```

4. Instale o certificado raiz em sua CA privada usando o `import-certificate-authority-certificate` AWS CLI comando.

```
$ aws acm-pca import-certificate-authority-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --certificate file://rootCA.pem --region aws-region
```

Gerar e exportar o certificado do sistema de arquivos e do cliente

1. Use o `request-certificate` AWS CLI comando para solicitar um AWS Certificate Manager certificado para usar em seu sistema de arquivos e clientes.

```
$ aws acm request-certificate \
    --domain-name *.ec2.internal \
    --idempotency-token 12345 \
    --region aws-region \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

   Se a solicitação for bem-sucedida, o ARN do certificado emitido será retornado.

2. Por segurança, você deve atribuir uma frase-senha para a chave privada ao exportá-la. Crie uma frase-senha e armazene-a em um arquivo chamado `passphrase.txt`

3. Use o `export-certificate` AWS CLI comando para exportar o certificado privado emitido anteriormente. O arquivo exportado contém o certificado, a cadeia de certificados e a chave RSA privada criptografada de 2048 bits associada à chave pública incorporada ao certificado. Por segurança, você deve atribuir uma frase-senha para a chave privada ao exportá-la. O exemplo a seguir é para uma EC2 instância do Linux.

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
     --passphrase $(cat passphrase.txt | base64) --region aws-region >
 exported_cert.json
```

4. Use os comandos `jq` a seguir para extrair a chave privada e o certificado da resposta JSON.

```
$ passphrase=$(cat passphrase.txt | base64)
cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
```

5. Use os comandos `openssl` a seguir para decriptografar a chave privada da resposta JSON. Depois de inserir o comando, você será solicitado a digitar a frase-senha.

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

Instalando e configurando o Libreswan em IPsec um cliente Amazon Linux 2

As seções a seguir fornecem instruções para instalar e configurar o Libreswan em IPsec uma instância da Amazon EC2 executando o Amazon Linux 2.

Instalar e configurar o Libreswan

1. Conecte-se à sua EC2 instância usando SSH. Para obter instruções específicas sobre como fazer isso, consulte Conectar-se à instância do Linux usando um cliente SSH no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux..
2. Execute o comando a seguir para instalar o `libreswan`:

```
$ sudo yum install libreswan
```

3. (Opcional) Ao verificar IPsec em uma etapa posterior, essas propriedades podem ser sinalizadas sem essas configurações. Sugerimos testar sua instalação primeiro sem essas configurações. Se sua conexão tiver problemas, retorne a esta etapa e faça as alterações a seguir.

   Após a conclusão da instalação, use seu editor de texto preferencial para adicionar as entradas a seguir ao arquivo `/etc/sysctl.conf`.

```
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
```

```
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
```

Salve as alterações e saia do editor de texto.

4. Aplique as alterações:

```
$ sudo sysctl -p
```

5. Verifique a IPsec configuração.

```
$ sudo ipsec verify
```

Verifique se a versão do `Libreswan` que você instalou está em execução.

6. Inicialize o banco de dados IPsec NSS.

```
$ sudo ipsec checknss
```

Instalar o certificado no cliente

1. Copie o certificado que você gerou para o cliente no diretório de trabalho na EC2 instância. Você
2. Exporte o certificado gerado anteriormente em um formato compatível com o `libreswan`.

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \
    -certfile rootCA.pem -out certkey.p12 -name fsx
```

3. Importe a chave reformatada, fornecendo a frase-senha quando solicitado.

```
$ sudo ipsec import certkey.p12
```

4. Crie um arquivo IPsec de configuração usando o editor de texto preferido.

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

Adicione as seguintes entradas ao arquivo de configuração:

```
conn fsxn
    authby=rsasig
```

```
    left=172.31.77.6
    right=198.19.254.13
    auto=start
    type=transport
    ikev2=insist
    keyexchange=ike
    ike=aes256-sha2_384;dh20
    esp=aes_gcm_c256
    leftcert=fsx
    leftrsasigkey=%cert
    leftid=%fromcert
    rightid=%fromcert
    rightrsasigkey=%cert
```

Você iniciará IPsec no cliente após a configuração IPsec em seu sistema de arquivos.

Configurando IPsec em seu sistema de arquivos

Esta seção fornece instruções sobre como instalar o certificado em seu sistema de arquivos FSx para ONTAP e IPsec configurá-lo.

Instalar o certificado no sistema de arquivos

1. Copie os arquivos do certificado raiz (`rootCA.pem`)), do certificado do cliente (`cert.pem`) e da chave decriptografada (`decrypted.key`) para o sistema de arquivos. Você precisará saber a senha do certificado.
2. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.
3. Use cat em um cliente (não no sistema de arquivos) para listar o conteúdo dos arquivos `rootCA.pem`, `cert.pem` e `decrypted.key` para que você possa copiar a saída de cada arquivo e colá-la quando solicitado nas etapas a seguir.

   ```
   $ > cat cert.pem
   ```

Copie o conteúdo do certificado.

4. Você deve instalar todos os certificados de CA usados durante a autenticação mútua, incluindo tanto do lado do ONTAP quanto do lado do cliente, no gerenciamento de ONTAP certificados CAs, a menos que ele já esteja instalado (como é o caso de uma CA raiz autoassinada do ONTAP).

   Use o comando `security certificate install` NetApp CLI da seguinte forma para instalar o certificado do cliente:

   ```
   FSxID123:: > security certificate install -vserver dr -type client -cert-name
    ipsec-client-cert
   ```

   ```
   Please enter Certificate: Press <Enter> when done
   ```

   Cole o conteúdo do arquivo `cert.pem` que você copiou anteriormente e pressione Enter.

   ```
   Please enter Private Key: Press <Enter> when done
   ```

   Cole o conteúdo do arquivo `decrypted.key` e pressione Enter.

   ```
   Do you want to continue entering root and/or intermediate certificates {y|n}:
   ```

   Insira n para concluir a inserção do certificado do cliente.

5. Crie e instale um certificado para uso da SVM. A CA emissora desse certificado já deve estar instalada ONTAP e adicionada. IPsec

   Use o seguinte comando para instalar o certificado raiz:

   ```
   FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
    ipsec-ca-cert
   ```

   ```
   Please enter Certificate: Press <Enter> when done
   ```

   Cole o conteúdo do arquivo `rootCA.pem` e pressione Enter.

6. Para garantir que a CA instalada esteja dentro do caminho de busca da IPsec CA durante a autenticação, adicione o gerenciamento de ONTAP certificados CAs ao IPsec módulo usando o comando “security ipsec ca-certificate add”.

   Digite o seguinte comando para adicionar o certificado raiz:

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. Digite o comando a seguir para criar a IPsec política necessária no banco de dados de políticas de segurança (SPD).

```
security ipsec policy create -vserver dr -name policy-name -local-ip-
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
 ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
 "CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. Use o comando a seguir para mostrar a IPsec política para confirmação do sistema de arquivos.

```
FSxID123:: > security ipsec policy show -vserver dr -instance

                                 Vserver: dr
                             Policy Name: promise
                      Local IP Subnets: 198.19.254.13/32
                     Remote IP Subnets: 172.31.0.0/16
                           Local Ports: 0-0
                          Remote Ports: 0-0
                             Protocols: any
                                Action: ESP_TRA
                          Cipher Suite: SUITEB_GCM256
   IKE Security Association Lifetime: 86400
  IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
                    Is Policy Enabled: true
                       Local Identity: CN=*.ec2.internal
                      Remote Identity: CN=*.ec2.internal
                Authentication Method: PKI
      Certificate for Local Identity: ipsec-client-cert
```

Comece IPsec com o cliente

Agora IPsec está configurado no sistema FSx de arquivos ONTAP e no cliente, você pode começar IPsec no cliente.

1. Conecte-se ao sistema do cliente usando SSH.
2. Começar IPsec.

```
$ sudo ipsec start
```

3. Verifique o status do IPsec.

```
$ sudo ipsec status
```

4. Monte um volume no sistema de arquivos.

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. Verifique a IPsec configuração mostrando a conexão criptografada em seu sistema de arquivos FSx para ONTAP.

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ---------------- -----------
dr          policy-name
                   198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                   198.19.254.38   172.31.65.193   4fd3f22c993e60c5 ESTABLISHED
2 entries were displayed.
```

Configuração IPsec para vários clientes

Quando um pequeno número de clientes precisa aproveitar IPsec, usar uma única entrada SPD para cada cliente é suficiente. No entanto, quando centenas ou até milhares de clientes precisarem aproveitar IPsec, recomendamos que você use a configuração de IPsec vários clientes.

FSx for ONTAP suporta a conexão de vários clientes em várias redes a um único endereço IP SVM com IPsec habilitado. Você pode fazer isso usando a configuração `subnet` ou `Allow all clients`, que são explicadas nos seguintes procedimentos:

Para configurar IPsec para vários clientes usando uma configuração de sub-rede

Para permitir que todos os clientes de uma sub-rede específica (192.168.134.0/24, por exemplo) se conectem a um único endereço IP da SVM usando uma única entrada de política SPD, especifique `remote-ip-subnets` no formulário da sub-rede. Além disso, especifique o campo `remote-identity` com a identidade correta no lado do cliente.

> **Important**
>
> Ao usar a autenticação de certificado, cada cliente pode usar seu próprio certificado exclusivo ou um certificado compartilhado para se autenticar. FSx for ONTAP IPsec verifica a validade do certificado com base no CAs instalado em seu armazenamento confiável local. FSx para ONTAP também suporta a verificação da lista de revogação de certificados (CRL).

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Use o comando `security ipsec policy create` NetApp ONTAP CLI da seguinte forma, substituindo os *`sample`* valores pelos seus valores específicos.

   ```
   FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
     -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
     -local-ports 2049 -protocols tcp -auth-method PSK \
     -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
     -remote-identity client_side_identity
   ```

Para configurar IPsec para vários clientes usando uma configuração de permitir todos os clientes

Para permitir que qualquer cliente, independentemente do endereço IP de origem, se conecte ao endereço IP IPsec habilitado para SVM, use o `0.0.0.0/0` curinga ao especificar o campo. `remote-ip-subnets`

Além disso, especifique o campo `remote-identity` com a identidade correta no lado do cliente. No caso da autenticação de certificado, você pode digitar `ANYTHING`.

Além disso, quando o curinga 0.0.0.0/0 é usado, você deve configurar um número de porta local ou remota específico para uso. Por exemplo, porta NFS 2049.

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Use o comando `security ipsec policy create` NetApp ONTAP CLI da seguinte forma, substituindo os *`sample`* valores pelos seus valores específicos.

   ```
   FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
     -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
     -local-ports 2049 -protocols tcp -auth-method PSK \
     -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
     -local-ports 2049 -remote-identity client_side_identity
   ```

Gerenciamento de identidade e acesso da Amazon FSx para NetApp ONTAP

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar

os recursos da Amazon FSx . O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como o Amazon FSx for NetApp ONTAP funciona com o IAM
- Exemplos de políticas baseadas em identidade para Amazon for ONTAP FSx NetApp
- Solução de problemas de identidade e acesso ao Amazon FSx for NetApp ONTAP
- Usando funções vinculadas a serviços para a Amazon FSx
- Usando tags com a Amazon FSx

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz na Amazon FSx.

Usuário do serviço — Se você usa o FSx serviço da Amazon para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais FSx recursos da Amazon para fazer seu trabalho, você pode precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se você não conseguir acessar um recurso na Amazon FSx, consulteSolução de problemas de identidade e acesso ao Amazon FSx for NetApp ONTAP.

Administrador de serviços — Se você é responsável pelos FSx recursos da Amazon em sua empresa, provavelmente tem acesso total à Amazon FSx. É seu trabalho determinar quais FSx recursos e recursos da Amazon seus usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM com a Amazon FSx, consulteComo o Amazon FSx for NetApp ONTAP funciona com o IAM.

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso à Amazon FSx. Para ver exemplos de políticas FSx baseadas

em identidade da Amazon que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para Amazon for ONTAP FSx NetApp

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais

do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários

têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode alternar de um usuário para uma função do IAM (console). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.

- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
- Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível ao armazenamento de chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais

informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal

especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.

- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o Amazon FSx for NetApp ONTAP funciona com o IAM

Antes de usar o IAM para gerenciar o acesso à Amazon FSx, saiba quais recursos do IAM estão disponíveis para uso com a Amazon FSx.

Recursos do IAM que você pode usar com a Amazon FSx para NetApp ONTAP

Recurso do IAM	FSx Suporte da Amazon
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim

Recurso do IAM	FSx Suporte da Amazon
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para ter uma visão de alto nível de como a Amazon FSx e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para a Amazon FSx

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para a Amazon FSx

Para ver exemplos de políticas FSx baseadas em identidade da Amazon, consulte. Exemplos de políticas baseadas em identidade para Amazon for ONTAP FSx NetApp

Políticas baseadas em recursos na Amazon FSx

Compatibilidade com políticas baseadas em recursos: não

Ações políticas para a Amazon FSx

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de FSx ações da Amazon, consulte Ações definidas pela Amazon FSx na Referência de autorização de serviço.

As ações políticas na Amazon FSx usam o seguinte prefixo antes da ação:

```
fsx
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Para ver exemplos de políticas FSx baseadas em identidade da Amazon, consulte. Exemplos de políticas baseadas em identidade para Amazon for ONTAP FSx NetApp

Recursos de políticas para a Amazon FSx

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de FSx recursos da Amazon e seus ARNs, consulte Recursos definidos pela Amazon FSx na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pela Amazon. FSx

Para ver exemplos de políticas FSx baseadas em identidade da Amazon, consulte. Exemplos de políticas baseadas em identidade para Amazon for ONTAP FSx NetApp

Chaves de condição de política para a Amazon FSx

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você

especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de FSx condição da Amazon, consulte Chaves de condição da Amazon FSx na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pela Amazon FSx.

Para ver exemplos de políticas FSx baseadas em identidade da Amazon, consulte. Exemplos de políticas baseadas em identidade para Amazon for ONTAP FSx NetApp

Listas de controle de acesso (ACLs) na Amazon FSx

Suportes ACLs: Não

Controle de acesso baseado em atributos (ABAC) com a Amazon FSx

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Para obter mais informações sobre a marcação de FSx recursos da Amazon, consulteMarcação de recursos da Amazon FSx .

Para visualizar um exemplo de política baseada em identidade para limitar o acesso a um recurso baseado em tags desse recurso, consulte Usando tags para controlar o acesso aos seus FSx recursos da Amazon.

Usando credenciais temporárias com a Amazon FSx

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil do IAM (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para a Amazon FSx

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um

serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço para a Amazon FSx

Compatível com perfis de serviço: não

Funções vinculadas a serviços para a Amazon FSx

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.

Para obter detalhes sobre como criar ou gerenciar funções FSx vinculadas a serviços da Amazon, consulte. Usando funções vinculadas a serviços para a Amazon FSx

Exemplos de políticas baseadas em identidade para Amazon for ONTAP FSx NetApp

Por padrão, usuários e funções não têm permissão para criar ou modificar FSx recursos da Amazon. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pela Amazon FSx, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para a Amazon FSx na Referência de Autorização de Serviço. ARNs

Tópicos

- Práticas recomendadas de política
- Usando o FSx console da Amazon
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir FSx recursos da Amazon em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usando o FSx console da Amazon

Para acessar o console Amazon FSx for NetApp ONTAP, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os FSx recursos da Amazon em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o FSx console da Amazon, anexe também a política `AmazonFSxConsoleReadOnlyAccess` AWS gerenciada às entidades. Para obter informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Você pode ver as `AmazonFSxConsoleReadOnlyAccess` e outras políticas de serviços FSx gerenciados da Amazon emAWS políticas gerenciadas para Amazon FSx for OpenZFS.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solução de problemas de identidade e acesso ao Amazon FSx for NetApp ONTAP

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com a Amazon FSx e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação na Amazon FSx
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas de fora da minha Conta da AWS acessem meus FSx recursos da Amazon

Não estou autorizado a realizar uma ação na Amazon FSx

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `fsx:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `fsx:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para a Amazon FSx.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação na Amazon FSx. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas de fora da minha Conta da AWS acessem meus FSx recursos da Amazon

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se a Amazon FSx oferece suporte a esses recursos, consulteComo o Amazon FSx for NetApp ONTAP funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Usando funções vinculadas a serviços para a Amazon FSx

A Amazon FSx usa AWS Identity and Access Management funções vinculadas a serviços (IAM). Uma função vinculada a serviços é um tipo exclusivo de função do IAM vinculada diretamente à Amazon. FSx As funções vinculadas ao serviço são predefinidas pela Amazon FSx e incluem todas as permissões que o serviço exige para ligar para outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração da Amazon FSx porque você não precisa adicionar manualmente as permissões necessárias. A Amazon FSx define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente a Amazon FSx pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus FSx recursos da Amazon porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços suportados por perfis vinculados a serviços, consulte Serviços da AWS Suportados pelo IAM e procure os serviços que apresentarem Sim na coluna Função Vinculada a Serviço.. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Permissões de função vinculadas ao serviço para a Amazon FSx

A Amazon FSx usa a função vinculada ao serviço chamada AWSServiceRoleForAmazonFSx— Que executa determinadas ações em sua conta, como criar interfaces de rede elástica para seus sistemas de arquivos em sua VPC e publicar métricas de volume e sistema de arquivos em. CloudWatch

Para as atualizações dessa política, consulte Amazon FSx ServiceRolePolicy.

Detalhes das permissões

Detalhes das permissões

As permissões de AWSService RoleForAmazon FSx função são definidas pela política FSx ServiceRolePolicy AWS gerenciada da Amazon. O AWSService RoleForAmazon FSx tem as seguintes permissões:

> **Note**
>
> O AWSService RoleForAmazon FSx é usado por todos os tipos de sistema de FSx arquivos da Amazon; algumas das permissões listadas não se aplicam ao FSx ONTAP.

- `ds`— Permite que FSx a Amazon visualize, autorize e não autorize aplicativos em seu diretório. AWS Directory Service
- `ec2`— Permite que FSx a Amazon faça o seguinte:
  - Visualize, crie e desassocie interfaces de rede associadas a um sistema de FSx arquivos da Amazon.
  - Visualize um ou mais endereços IP elásticos associados a um sistema de FSx arquivos da Amazon.

  - Veja a Amazon VPCs, os grupos de segurança e as sub-redes associadas a um sistema de FSx arquivos da Amazon.
  - Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança passíveis de uso com uma VPC.
  - Crie uma permissão para que um usuário AWS autorizado realize determinadas operações em uma interface de rede.
- `cloudwatch`— Permite que FSx a Amazon publique pontos de dados métricos CloudWatch sob o FSx namespace AWS//.
- `route53`— Permite que FSx a Amazon associe uma Amazon VPC a uma zona hospedada privada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
```

```
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
```

```
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        }
    ]
}
```

Todas as atualizações dessa política estão descritas em FSx Atualizações da Amazon para políticas AWS gerenciadas.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Criação de uma função vinculada a serviços para a Amazon FSx

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria um sistema de arquivos na CLI do IAM ou na API do IAM, a Amazon FSx cria a função vinculada ao serviço para você. AWS Management Console

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Para saber mais, consulte Uma Nova Função Apareceu na minha Conta do IAM.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você pode usar esse mesmo processo para recriar a função na sua conta. Quando você cria um sistema de arquivos, a Amazon FSx cria a função vinculada ao serviço para você novamente.

Editando uma função vinculada ao serviço para a Amazon FSx

FSx A Amazon não permite que você edite a função AWSService RoleForAmazon FSx vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para a Amazon FSx

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve excluir todos os seus sistemas de arquivos e backups para poder excluir manualmente o perfil vinculado ao serviço.

> **Note**
>
> Se o FSx serviço da Amazon estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console, a CLI ou a API do IAM para excluir a função vinculada ao serviço AWSServiceRoleForAmazonFSx. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas a FSx serviços da Amazon

A Amazon FSx oferece suporte ao uso de funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Para mais informações, consulte Regiões e endpoints da AWS.

Usando tags com a Amazon FSx

Você pode usar tags para controlar o acesso aos FSx recursos da Amazon e implementar o controle de acesso baseado em atributos (ABAC). Para aplicar tags aos FSx recursos da Amazon durante a criação, os usuários devem ter determinadas permissões AWS Identity and Access Management (IAM).

Conceder permissão para marcar recursos durante a criação

Com algumas ações de API da FSx Amazon que criam recursos, você pode especificar tags ao criar o recurso. É possível usar essas tags de recurso para implementar o controle de acesso por atributo (ABAC). Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

Para permitir que os usuários marquem recursos na criação, eles devem ter permissão para usar a ação que cria o recurso, como `fsx:CreateFileSystem`, `fsx:CreateStorageVirtualMachine` ou `fsx:CreateVolume`. Se tags forem especificadas na ação de criação do recurso, o IAM executará autorização adicional na ação `fsx:TagResource` para verificar se os usuários têm permissões para criar tags. Portanto, os usuários também precisam ter permissões para usar a ação `fsx:TagResource`.

O exemplo de política a seguir permite que os usuários criem sistemas de arquivos e máquinas virtuais de armazenamento (SVMs) e apliquem tags a eles durante a criação em um local específico Conta da AWS.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:CreateStorageVirtualMachine",
         "fsx:TagResource"
      ],
      "Resource": [
```

```
            "arn:aws:fsx:region:account-id:file-system/*",
            "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
        ]
      }
    ]
}
```

Da mesma forma, a política a seguir permite que os usuários criem backups em um sistema de arquivos específico e apliquem qualquer tag ao backup durante a criação do backup.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

A ação `fsx:TagResource` só será avaliada se as tags forem aplicadas durante a ação de criação do recurso. Portanto, um usuário que tiver permissões para criar um recurso (supondo que não existam condições de tag) não precisará de permissão para usar a ação `fsx:TagResource` se nenhuma tag for especificada na solicitação. Contudo, se o usuário tentar criar um recurso com tags, haverá falha na solicitação se o usuário não tiver permissão para usar a ação `fsx:TagResource`.

Para obter mais informações sobre a marcação de FSx recursos da Amazon, consulteMarcação de recursos da Amazon FSx . Para obter mais informações sobre o uso de tags para controlar o acesso aos FSx recursos da Amazon, consulteUsando tags para controlar o acesso aos seus FSx recursos da Amazon.

Usando tags para controlar o acesso aos seus FSx recursos da Amazon

Para controlar o acesso aos FSx recursos e ações da Amazon, você pode usar políticas do IAM com base em tags. É possível conceder o controle de duas formas:

- Você pode controlar o acesso aos FSx recursos da Amazon com base nas tags desses recursos.
- Controlar quais tags podem ser transmitidas em uma condição de solicitação do IAM.

Para obter informações sobre como usar tags para controlar o acesso aos AWS recursos, consulte Como controlar o acesso usando tags no Guia do usuário do IAM. Para obter mais informações sobre a marcação de FSx recursos da Amazon no momento da criação, consulteConceder permissão para marcar recursos durante a criação. Para obter mais informações sobre como marcar recursos, consulte Marcação de recursos da Amazon FSx .

Como controlar o acesso com base em tags em um recurso

Para controlar quais ações um usuário ou função pode realizar em um FSx recurso da Amazon, você pode usar tags no recurso. Por exemplo, talvez você queira permitir ou negar operações de API específicas em um recurso do sistema de arquivos com base no par chave-valor da tag no recurso.

Example Exemplo de política: criar um sistema de arquivos somente quando uma tag específica for usada

Essa política permite que o usuário só crie um sistema de arquivos quando o marcar com um par de chave/valor de tag específico, neste exemplo, `key=Department`, `value=Finance`.

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example Exemplo de política — Crie backups somente dos volumes Amazon FSx for NetApp ONTAP com uma tag específica

Essa política permite que os usuários criem backups somente FSx para volumes ONTAP marcados com o par de valores-chave,. `key=Department` `value=Finance` O backup é criado com a tag `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example Exemplo de política: criar um volume com uma tag específica usando backups com uma tag específica

Essa política só permite que os usuários criem volumes marcados com `Department=Finance` usando backups marcados com `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Exemplo de política: excluir sistemas de arquivos com tags específicas

Essa política só permite que o usuário exclua sistemas de arquivos marcados com `Department=Finance`. Se um backup final for criado, ele deverá ser marcado com `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Exemplo de política: excluir um volume com tags específicas

Essa política só permite que o usuário exclua volumes marcados com `Department=Finance`. Se um backup final for criado, ele deverá ser marcado com `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
```

```
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

AWS políticas gerenciadas para Amazon FSx for OpenZFS

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Amazon FSx ServiceRolePolicy

Permite que FSx a Amazon gerencie AWS recursos em seu nome. Para saber mais, consulte Usando funções vinculadas a serviços para a Amazon FSx.

AWS política gerenciada: Amazon FSx DeleteServiceLinkedRoleAccess

Não é possível anexar a `AmazonFSxDeleteServiceLinkedRoleAccess` às entidades do IAM. Essa política está vinculada a um serviço e só é usada com o perfil vinculado a esse serviço. Você não pode anexar, desanexar, modificar ou excluir essa política. Para obter mais informações, consulte Usando funções vinculadas a serviços para a Amazon FSx.

Essa política concede permissões administrativas que permitem FSx à Amazon excluir sua função vinculada ao serviço para acesso ao Amazon S3, usada somente FSx pelo Amazon for Lustre.

Detalhes das permissões

Essa política inclui permissões `iam` para permitir que FSx a Amazon visualize, exclua e visualize o status de exclusão das funções vinculadas ao FSx serviço para acesso ao Amazon S3.

Para ver as permissões dessa política, consulte a Amazon FSx DeleteServiceLinkedRoleAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: Amazon FSx FullAccess

Você pode anexar FSx FullAccess a Amazon às suas entidades do IAM. A Amazon FSx também atribui essa política a uma função de serviço que permite FSx à Amazon realizar ações em seu nome.

Fornece acesso total à Amazon FSx e acesso aos AWS serviços relacionados.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`— Permite que os diretores tenham acesso total para realizar todas as FSx ações da Amazon, exceto a. `BypassSnaplockEnterpriseRetention`
- `ds`— Permite que os diretores visualizem informações sobre os AWS Directory Service diretórios.
- `ec2`
  - Permite que as entidades principais criem tags sob as condições especificadas.

  - Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança passíveis de uso com uma VPC.
- `iam`— Permite que os princípios criem uma função vinculada ao FSx serviço da Amazon em nome do usuário. Isso é necessário para que a Amazon FSx possa gerenciar AWS recursos em nome do usuário.
- `firehose`: permite que as entidades principais gravem registros em um Amazon Data Firehose. Isso é necessário FSx para que os usuários possam monitorar o acesso ao sistema de arquivos do Windows File Server enviando registros de acesso de auditoria para o Firehose.
- `logs`: permite que as entidades principais criem grupos de logs, fluxos de logs e gravem eventos nos fluxos de logs. Isso é necessário FSx para que os usuários possam monitorar o acesso ao sistema de arquivos do Windows File Server enviando registros de acesso de auditoria para o CloudWatch Logs.

Para ver as permissões dessa política, consulte a Amazon FSx FullAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: Amazon FSx ConsoleFullAccess

É possível anexar a política `AmazonFSxConsoleFullAccess` às identidades do IAM.

Esta política concede permissões administrativas que permitem acesso total à Amazon FSx e acesso a AWS serviços relacionados por meio do AWS Management Console.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`— Permite que os diretores realizem todas as ações no console FSx de gerenciamento da Amazon, exceto`BypassSnaplockEnterpriseRetention`.
- `cloudwatch`— Permite que os diretores visualizem CloudWatch alarmes e métricas no console de FSx gerenciamento da Amazon.
- `ds`— Permite que os diretores listem informações sobre um AWS Directory Service diretório.
- `ec2`
  - Permite que os diretores criem tags em tabelas de rotas, listem interfaces de rede, tabelas de rotas, grupos de segurança, sub-redes e a VPC associada a um sistema de arquivos da Amazon. FSx

  - Permite que os diretores forneçam validação aprimorada do grupo de segurança de todos os grupos de segurança que podem ser usados com uma VPC.
  - Permite que os diretores visualizem as interfaces de rede elásticas associadas a um sistema de FSx arquivos da Amazon.
- `kms`— Permite que os diretores listem aliases para AWS Key Management Service chaves.
- `s3`: permite que as entidades principais listem alguns ou todos os objetos em um bucket do Amazon S3 (até mil).
- `iam`— Concede permissão para criar uma função vinculada ao serviço que permite FSx à Amazon realizar ações em nome do usuário.

Para ver as permissões dessa política, consulte a Amazon FSx ConsoleFullAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: Amazon FSx ConsoleReadOnlyAccess

É possível anexar a política `AmazonFSxConsoleReadOnlyAccess` às identidades do IAM.

Esta política concede permissões somente de leitura à Amazon FSx e aos AWS serviços relacionados para que os usuários possam visualizar informações sobre esses serviços no. AWS Management Console

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`— Permite que os diretores visualizem informações sobre os sistemas de FSx arquivos da Amazon, incluindo todas as tags, no Amazon FSx Management Console.
- `cloudwatch`— Permite que os diretores visualizem CloudWatch alarmes e métricas no Amazon FSx Management Console.
- `ds`— Permite que os diretores visualizem informações sobre um AWS Directory Service diretório no Amazon FSx Management Console.
- `ec2`
  - Permite que os diretores visualizem interfaces de rede, grupos de segurança, sub-redes e a VPC associada a um FSx sistema de arquivos da Amazon no Amazon Management Console. FSx

  - Permite que os diretores forneçam validação aprimorada do grupo de segurança de todos os grupos de segurança que podem ser usados com uma VPC.
  - Permite que os diretores visualizem as interfaces de rede elásticas associadas a um sistema de FSx arquivos da Amazon.
- `kms`— Permite que os diretores visualizem aliases para AWS Key Management Service chaves no Amazon FSx Management Console.
- `log`— Permite que os diretores descrevam os grupos de log do Amazon CloudWatch Logs associados à conta que fez a solicitação. Isso é necessário para que os diretores possam visualizar a configuração de auditoria de acesso a arquivos existente FSx para um sistema de arquivos do Windows File Server.
- `firehose`: permite que as entidades principais descrevam os fluxos de entrega do Amazon Data Firehose associados à conta que está fazendo a solicitação. Isso é necessário para que os diretores possam visualizar a configuração de auditoria de acesso a arquivos existente FSx para um sistema de arquivos do Windows File Server.

Para ver as permissões dessa política, consulte a Amazon FSx ConsoleReadOnlyAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: Amazon FSx ReadOnlyAccess

É possível anexar a política `AmazonFSxReadOnlyAccess` às identidades do IAM.

- `fsx`— Permite que os diretores visualizem informações sobre os sistemas de FSx arquivos da Amazon, incluindo todas as tags, no Amazon FSx Management Console.
- `ec2`: fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança passíveis de uso com uma VPC.

Para ver as permissões dessa política, consulte a Amazon FSx ReadOnlyAccess no Guia de referência de políticas AWS gerenciadas.

FSx Atualizações da Amazon para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas da Amazon FSx desde que esse serviço começou a monitorar essas mudanças. Para receber alertas automáticos sobre alterações nesta página, assine o feed RSS na FSx Histórico de documentos da Amazon FSx para NetApp ONTAP página da Amazon.

Alteração	Descrição	Data
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `fsx:CreateAndAttachS3AccessPoint` que permite aos diretores criar um S3 e anexá-lo a um FSx volume.	14 de abril de 2025
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `fsx:DescribeS3AccessPointAttachments` que permite aos diretores listar todos os S3 em um Conta da AWS Região da AWS	14 de abril de 2025
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `fsx:UpdateS3AccessPointAttachments` que permite que os diretores modifiquem um S3 existente.	14 de abril de 2025
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `fsx:DetachAndDeleteS3AccessPoint` que permite que os diretores excluam um S3.	14 de abril de 2025
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `fsx:CreateAndAttachS3AccessPoint` que permite aos diretores criar um S3 e anexá-lo a um FSx volume.	14 de abril de 2025

Alteração	Descrição	Data
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `fsx:DescribeS3AccessPointAttachments` que permite aos diretores listar todos os S3 em um Conta da AWS Região da AWS	14 de abril de 2025
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `fsx:UpdateS3AccessPointAttachments` que permite que os diretores modifiquem um S3 existente.	14 de abril de 2025
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `fsx:DetachAndDeleteS3AccessPoint` que permite que os diretores excluam um S3.	14 de abril de 2025
Amazon FSx ConsoleReadOnlyAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `ec2:DescribeNetworkInterfaces` que permite que os diretores visualizem as interfaces de rede elásticas associadas ao sistema de arquivos.	25 de fevereiro de 2025

Alteração	Descrição	Data
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `ec2:DescribeNetworkInterfaces` que permite que os diretores visualizem as interfaces de rede elásticas associadas ao sistema de arquivos.	07 de fevereiro de 2025
Amazon FSx ServiceRolePolicy — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	9 de janeiro de 2024
Amazon FSx ReadOnlyAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	9 de janeiro de 2024

Alteração	Descrição	Data
Amazon FSx ConsoleReadOnlyAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	9 de janeiro de 2024
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	9 de janeiro de 2024
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	9 de janeiro de 2024

Alteração	Descrição	Data
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação de dados entre regiões e entre contas FSx para sistemas de arquivos OpenZFS.	20 de dezembro de 2023
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação de dados entre regiões e entre contas FSx para sistemas de arquivos OpenZFS.	20 de dezembro de 2023
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação sob demanda de volumes FSx para sistemas de arquivos OpenZFS.	26 de novembro de 2023
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação sob demanda de volumes FSx para sistemas de arquivos OpenZFS.	26 de novembro de 2023

Alteração	Descrição	Data
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que os usuários visualizem, habilitem e desabilitem o suporte compartilhado de VPC FSx para sistemas de arquivos ONTAP Multi-AZ.	14 de novembro de 2023
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que os usuários visualizem, habilitem e desabilitem o suporte compartilhado de VPC FSx para sistemas de arquivos ONTAP Multi-AZ.	14 de novembro de 2023
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon gerencie configurações de rede FSx para sistemas de arquivos OpenZFS Multi-AZ.	9 de agosto de 2023
AWS política gerenciada: Amazon FSx ServiceRolePolicy — Atualização de uma política existente	A Amazon FSx modificou a `cloudwatch:PutMetricData` permissão existente para que a Amazon FSx publique CloudWatch métricas no `AWS/FSx` namespace.	24 de julho de 2023

Alteração	Descrição	Data
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx atualizou a política para remover a `fsx:*` permissão e adicionar `fsx` ações específicas.	13 de julho de 2023
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx atualizou a política para remover a `fsx:*` permissão e adicionar `fsx` ações específicas.	13 de julho de 2023
Amazon FSx ConsoleReadOnlyAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que os usuários visualizem métricas de desempenho aprimoradas e ações recomendadas FSx para sistemas de arquivos do Windows File Server no FSx console da Amazon.	21 de setembro de 2022
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que os usuários visualizem métricas de desempenho aprimoradas e ações recomendadas FSx para sistemas de arquivos do Windows File Server no FSx console da Amazon.	21 de setembro de 2022
Amazon FSx ReadOnlyAccess — Iniciou a política de rastreamento	Essa política concede acesso somente para leitura a todos os FSx recursos da Amazon e a quaisquer tags associadas a eles.	4 de fevereiro de 2022

Alteração	Descrição	Data
Amazon FSx DeleteServiceLinkedRoleAccess — Iniciou a política de rastreamento	Essa política concede permissões administrativas que permitem FSx à Amazon excluir sua função vinculada ao serviço para acesso ao Amazon S3.	7 de janeiro de 2022
Amazon FSx ServiceRolePolicy — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon gerencie as configurações de rede dos sistemas de arquivos Amazon FSx for NetApp ONTAP.	2 de setembro de 2021
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon crie tags em tabelas de EC2 rotas para chamadas com escopo reduzido.	2 de setembro de 2021
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon crie sistemas de arquivos Amazon FSx for NetApp ONTAP Multi-AZ.	2 de setembro de 2021
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon crie tags em tabelas de EC2 rotas para chamadas com escopo reduzido.	2 de setembro de 2021

Alteração	Descrição	Data
Amazon FSx ServiceRolePolicy — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon descreva e grave nos fluxos de log do CloudWatch Logs. Isso é necessário para que os usuários possam visualizar registros de auditoria de acesso a arquivos FSx para sistemas de arquivos do Windows File Server usando CloudWatch Logs.	8 de junho de 2021
Amazon FSx ServiceRolePolicy — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon descreva e grave nos fluxos de entrega do Amazon Data Firehose. Isso é necessário para que os usuários possam visualizar os registros de auditoria de acesso aos arquivos de um sistema FSx de arquivos do Windows File Server usando o Amazon Data Firehose.	8 de junho de 2021

Alteração	Descrição	Data
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que os diretores descrevam e criem grupos de CloudWatch registros de registros, fluxos de registros e gravem eventos em fluxos de registros. Isso é necessário para que os diretores possam visualizar os registros de auditoria de acesso a arquivos FSx para sistemas de arquivos do Windows File Server usando CloudWatch Logs.	8 de junho de 2021
Amazon FSx FullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que os diretores descrevam e gravem registros em um Amazon Data Firehose. Isso é necessário para que os usuários possam visualizar os registros de auditoria de acesso aos arquivos de um sistema FSx de arquivos do Windows File Server usando o Amazon Data Firehose.	8 de junho de 2021

Alteração	Descrição	Data
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que os diretores descrevam os grupos de log do Amazon CloudWatch Logs associados à conta que fez a solicitação. Isso é necessário para que os diretores possam escolher um grupo de registros de CloudWatch registros existente ao configurar a auditoria de acesso a arquivos FSx para um sistema de arquivos do Windows File Server.	8 de junho de 2021
Amazon FSx ConsoleFullAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que os diretores descrevam os fluxos de entrega do Amazon Data Firehose associados à conta que fez a solicitação. Isso é necessário para que os diretores possam escolher um stream de entrega existente do Firehose ao configurar a auditoria de acesso a arquivos para FSx um sistema de arquivos do Windows File Server.	8 de junho de 2021

Alteração	Descrição	Data
Amazon FSx ConsoleReadOnlyAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que os diretores descrevam os grupos de log do Amazon CloudWatch Logs associados à conta que fez a solicitação. Isso é necessário para que os diretores possam visualizar a configuração de auditoria de acesso a arquivos existente FSx para um sistema de arquivos do Windows File Server.	8 de junho de 2021
Amazon FSx ConsoleReadOnlyAccess — Atualização de uma política existente	A Amazon FSx adicionou novas permissões para permitir que os diretores descrevam os fluxos de entrega do Amazon Data Firehose associados à conta que fez a solicitação. Isso é necessário para que os diretores possam visualizar a configuração de auditoria de acesso a arquivos existente FSx para um sistema de arquivos do Windows File Server.	8 de junho de 2021

Alteração	Descrição	Data
A Amazon FSx começou a monitorar as mudanças	A Amazon FSx começou a monitorar as mudanças em suas políticas AWS gerenciadas.	8 de junho de 2021

Controle de acesso ao sistema de arquivos com a Amazon VPC

Você acessa seus sistemas de arquivos Amazon FSx for NetApp ONTAP SVMs usando o nome DNS ou o endereço IP de um de seus endpoints, dependendo do tipo de acesso. O nome DNS é mapeado para o endereço IP privado da interface de rede elástica do sistema de arquivos ou da SVM na sua VPC. Somente recursos dentro da VPC associada, ou recursos conectados à VPC AWS Direct Connect ou VPN associada, podem acessar os dados em seu sistema de arquivos por meio dos protocolos NFS, SMB ou iSCSI. Para obter mais informações, consulte O que é a Amazon VPC? no Guia do usuário da Amazon VPC.

> **Warning**
>
> Você não deve modificar nem excluir as interfaces de rede elástica associadas ao seu sistema de arquivos. A modificação ou a exclusão da interface de rede pode causar uma perda permanente de conexão entre a VPC e o sistema de arquivos.

Grupos de segurança da Amazon VPC

Um grupo de segurança atua como um firewall virtual FSx para seus sistemas de arquivos ONTAP para controlar o tráfego de entrada e saída. As regras de entrada controlam o tráfego de entrada para o sistema de arquivos e as regras de saída controlam o tráfego de saída do sistema de arquivos. Ao criar um sistema de arquivos, você especifica a VPC na qual ele é criado e o grupo de segurança padrão dessa VPC é aplicado. Você pode adicionar regras a cada grupo de segurança que permitem o tráfego de ou para seus sistemas de arquivos associados SVMs e. É possível modificar as regras de um grupo de segurança a qualquer momento. As regras novas e modificadas são aplicadas automaticamente a todos os recursos associados ao grupo de segurança. Quando a Amazon FSx decide se permite que o tráfego chegue a um recurso, ela avalia todas as regras de todos os grupos de segurança associados ao recurso.

Para usar um grupo de segurança para controlar o acesso ao seu sistema de FSx arquivos da Amazon, adicione regras de entrada e saída. As regras de entrada controlam o tráfego de entrada e as regras de saída controlam o tráfego de saída do sistema de arquivos. Certifique-se de ter as regras de tráfego de rede corretas em seu grupo de segurança para mapear o compartilhamento de FSx arquivos do sistema de arquivos da Amazon em uma pasta na sua instância computacional compatível.

Para obter mais informações sobre regras de grupos de segurança, consulte Regras de grupos de segurança no Guia EC2 do usuário da Amazon.

Criar um grupo de segurança de VPC

Para criar um grupo de segurança para a Amazon FSx

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2.
2. No painel de navegação, escolha Grupos de segurança.
3. Escolha Create Security Group.
4. Especifique um nome e uma descrição para o grupo de segurança.
5. Para VPC, escolha a Amazon VPC associada ao seu sistema de arquivos para criar o grupo de segurança dentro dessa VPC.
6. Para regras de saída, permita todo o tráfego em todas as portas.
7. Adicione a regras a seguir às portas de entrada do grupo de segurança. Para o campo de origem, você deve escolher Personalizado e inserir os grupos de segurança ou os intervalos de endereços IP associados às instâncias que precisam acessar seu sistema FSx de arquivos do ONTAP, incluindo:

   - Clientes Linux, Windows e and/or macOS que acessam dados em seu sistema de arquivos via NFS, SMB ou iSCSI.
   - Qualquer arquivo ONTAP systems/clusters que você conectará ao seu sistema de arquivos (por exemplo, para usar SnapMirror SnapVault, ou FlexCache).
   - Qualquer cliente que você usará para acessar a API REST, CLI ZAPIs ou (por exemplo, Harvest/Grafana uma instância NetApp , Connector ou BlueXP) do ONTAP. NetApp

Protocolo	Portas	Função
Todos os ICMP	Todos	Como executar ping na instância

Protocolo	Portas	Função
SSH	22	Acesso SSH ao endereço IP da LIF de gerenciamento de cluster ou de uma LIF de gerenciamento de nós
TCP	111	Chamada de procedimento remoto para NFS
TCP	135	Chamada de procedimento remoto para CIFS
TCP	139	Sessão de serviço do NetBIOS para CIFS
TCP	161-162	Protocolo simples de gerenciamento de redes (SNMP)
TCP	443	Acesso da API REST do ONTAP ao endereço IP da LIF de gerenciamento de cluster ou de uma LIF de gerenciamento de SVM
TCP	445	Microsoft SMB/CIFS via TCP com enquadramento NetBIOS
TCP	635	Montagem NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS
TCP	3260	Acesso iSCSI por meio da LIF de dados do iSCSI
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status de rede para NFS
TCP	10000	Protocolo de gerenciamento de dados de rede (NDMP) e comunicação NetApp SnapMirror entre clusters
TCP	1104	Gerenciamento da comunicação NetApp SnapMirror entre clusters
TCP	11105	SnapMirror transferência de dados usando intercluster LIFs

Protocolo	Portas	Função
UDP	111	Chamada de procedimento remoto para NFS
UDP	135	Chamada de procedimento remoto para CIFS
UDP	137	Resolução de nomes do NetBIOS para CIFS
UDP	139	Sessão de serviço do NetBIOS para CIFS
UDP	161-162	Protocolo simples de gerenciamento de redes (SNMP)
UDP	635	Montagem NFS
UDP	2049	Daemon do servidor NFS
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status de rede para NFS
UDP	4049	Protocolo de cota NFS

8. Adicione o grupo de segurança à interface de rede elástica do sistema de arquivos.

Proibir acesso a um sistema de arquivos

Para proibir temporariamente o acesso de todos os clientes à rede ao seu sistema de arquivos, você pode remover todos os grupos de segurança associados à (s) interface (s) elástica (s) de rede do seu sistema de arquivos e substituí-los por um grupo sem inbound/outbound regras.

Validação de conformidade da Amazon FSx para NetApp ONTAP

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Governança e conformidade de segurança: esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- Referência de serviços qualificados para HIPAA: lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a HIPAA.
- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Amazon FSx para NetApp ONTAP e endpoints VPC de interface ()AWS PrivateLink

Você pode melhorar a postura de segurança da sua VPC configurando a FSx Amazon para usar uma interface VPC endpoint. Os endpoints VPC da Interface são alimentados por AWS PrivateLinkuma tecnologia que permite acessar a FSx APIs Amazon de forma privada sem um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect As instâncias em sua VPC não precisam de endereços IP públicos para se comunicar com a Amazon. FSx APIs O tráfego entre sua VPC e a Amazon FSx não sai da AWS rede.

Cada endpoint da VPC de interface é representado por uma ou mais interfaces de rede elástica em suas sub-redes. Uma interface de rede fornece um endereço IP privado que serve como ponto de entrada para o tráfego para a FSx API da Amazon. A Amazon FSx oferece suporte a endpoints VPC configurados com os tipos de IPv4 endereço IP Dualstack (IPv4 e). IPv6 Para obter mais informações, consulte Creating an interface VPC endpoint no Guia do usuário da Amazon VPC.

Considerações sobre os endpoints VPC da FSx interface Amazon

Antes de configurar uma interface VPC endpoint para a Amazon FSx, certifique-se de revisar as propriedades e limitações da interface VPC endpoint no Guia do usuário da Amazon VPC.

Você pode chamar qualquer uma das operações de FSx API da Amazon a partir da sua VPC. Por exemplo, você pode criar um sistema de arquivos FSx for ONTAP chamando a CreateFileSystem API de dentro da sua VPC. Para ver a lista completa da Amazon FSx APIs, consulte Ações na Referência de FSx API da Amazon.

Considerações sobre emparelhamento de VPC

Você pode conectar outras pessoas VPCs à VPC com endpoints de VPC de interface usando o peering de VPC. O peering de VPC é uma conexão de rede entre dois. VPCs Você pode estabelecer uma conexão de emparelhamento de VPC entre suas duas VPCs ou com uma VPC em outra. Conta da AWS Eles também VPCs podem estar em dois diferentes Regiões da AWS.

O tráfego entre os pares VPCs permanece na AWS rede e não atravessa a Internet pública. Depois de VPCs emparelhados, recursos como as instâncias do Amazon Elastic Compute Cloud EC2 (Amazon) em ambos VPCs podem acessar a FSx API da Amazon por meio de endpoints de VPC de interface criados em um dos. VPCs

Criação de uma interface VPC endpoint para a API da Amazon FSx

Você pode criar um VPC endpoint para a FSx API da Amazon usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para obter mais informações, consulte Creating an interface VPC endpoint no Guia do usuário da Amazon VPC.

Para criar uma interface VPC endpoint para a Amazon FSx, use uma das seguintes opções:

- **`com.amazonaws.`*`region`*`.fsx`**— Cria um endpoint para operações de FSx API da Amazon.
- **`com.amazonaws.`*`region`*`.fsx-fips`**— Cria um endpoint para a FSx API da Amazon que está em conformidade com o Federal Information Processing Standard (FIPS) 140-2.

Para usar a opção de DNS privado, é necessário definir os recursos `enableDnsHostnames` e `enableDnsSupport` da sua VPC. Para obter mais informações, consulte Viewing and updating DNS support for your VPC no Guia do usuário da Amazon VPC.

Exceto Regiões da AWS na China, se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para a Amazon com FSx o endpoint VPC usando seu nome DNS padrão para o, por exemplo. Região da AWS`fsx.us-east-1.amazonaws.com` Para a China (Pequim) e a China (Ningxia) Regiões da AWS, você pode fazer solicitações de API com o VPC endpoint `fsx-api.cn-north-1.amazonaws.com.cn` usando `fsx-api.cn-northwest-1.amazonaws.com.cn` e, respectivamente.

Para obter mais informações, consulte Accessing a service through an interface VPC endpoint no Guia do usuário da Amazon VPC.

Criação de uma política de VPC endpoint para a Amazon FSx

Para controlar o acesso à FSx API da Amazon, você pode anexar uma política AWS Identity and Access Management (IAM) ao seu VPC endpoint. A política especifica o seguinte:

- A entidade principal que pode realizar ações.
- As ações que podem ser realizadas.
- Os recursos aos quais as ações podem ser aplicadas.

Para mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Resiliência na Amazon FSx para ONTAP NetApp

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, a Amazon FSx oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Backup e restauração

FSx A Amazon cria e salva backups automatizados dos volumes em seu sistema de arquivos Amazon FSx for NetApp ONTAP. FSx A Amazon cria backups automatizados dos seus volumes durante a janela de backup do seu sistema de arquivos Amazon FSx for NetApp ONTAP. A Amazon FSx salva os backups automatizados de seus volumes de acordo com o período de retenção de backup que você especificar. Também é possível fazer backup dos volumes manualmente, criando um backup iniciado pelo usuário. Você restaura um backup de volume a qualquer momento criando um novo volume com o backup especificado como origem.

Para obter mais informações, consulte Proteger seus dados com backups de volume.

Snapshots

FSx A Amazon cria cópias instantâneas dos volumes Amazon FSx for NetApp ONTAP. Esses snapshots oferecem proteção contra exclusão ou modificação acidental de arquivos em seus volumes pelos usuários finais. Para obter mais informações, consulte Como proteger seus dados com snapshots.

Zonas de disponibilidade

Os sistemas de arquivos Amazon FSx for NetApp ONTAP foram projetados para fornecer disponibilidade contínua aos dados, mesmo no caso de uma falha no servidor. Cada sistema de

arquivos é alimentado por dois servidores de arquivos em pelo menos uma zona de disponibilidade, cada um com seu próprio armazenamento. A Amazon replica FSx automaticamente seus dados para protegê-los contra falhas de componentes, monitora continuamente as falhas de hardware e substitui automaticamente os componentes da infraestrutura em caso de falha. Os sistemas de arquivos são alternados automaticamente conforme necessário (normalmente em 60 segundos), e os clientes também são alternados automaticamente com o sistema de arquivos.

Sistemas de arquivos multi-AZ

Os sistemas de arquivos Amazon FSx for NetApp ONTAP são altamente disponíveis e duráveis em todas as zonas de AWS disponibilidade e foram projetados para fornecer disponibilidade contínua aos dados, mesmo no caso de uma zona de disponibilidade não estar disponível.

Para obter mais informações, consulte Opções de disponibilidade, durabilidade e implantação.

Sistemas de arquivos com uma única AZ

Os sistemas de arquivos Amazon FSx for NetApp ONTAP são altamente disponíveis e duráveis em uma única zona de AWS disponibilidade e foram projetados para fornecer disponibilidade contínua dentro dessa zona de disponibilidade no caso de falha de um servidor de arquivos ou disco individual.

Para obter mais informações, consulte Opções de disponibilidade, durabilidade e implantação.

Segurança de infraestrutura na Amazon FSx para NetApp ONTAP

Como um serviço gerenciado, o Amazon FSx for NetApp ONTAP é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar a Amazon FSx pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Use o NetApp ONTAP Vscan com FSx o ONTAP

Você pode usar o recurso NetApp ONTAP's Vscan para executar software antivírus de terceiros compatível. Para obter mais informações, consulte os seguintes recursos para cada uma das soluções com suporte:

- Deep Instinct — soluções de parceiros da Vscan e documentação do Deep Instinct 1
- SentinelOne — Soluções de parceiros Vscan e SentinelOne Singularity Cloud Data Security
- Symantec: soluções de parceiro Vscan e Symantec Protection Engine
- Trellix (anteriormente McAfee) — soluções de parceiros da Vscan e documentos de produtos da Trellix
- Trend Micro — soluções parceiras da Vscan

> **Note**
>
> [1] Você deve fazer login no portal do Deep Instinct para ver sua documentação.

Usuários e perfis do ONTAP

O NetApp ONTAP inclui uma capacidade de controle de acesso por perfil (RBAC) robusta e extensível. Os perfis do ONTAP definem os recursos e os privilégios do usuário ao utilizar a API REST e a CLI do ONTAP. Cada perfil define um nível diferente de recursos e privilégios administrativos. Você atribui funções aos usuários com o objetivo de controlar seu acesso aos FSx recursos do ONTAP ao usar a API ONTAP REST e a CLI. Há ONTAP funções disponíveis separadamente FSx para usuários do sistema de arquivos ONTAP e usuários de máquinas virtuais de armazenamento (SVM).

Quando você cria um sistema de arquivos FSx para ONTAP, um ONTAP usuário padrão é criado no nível do sistema de arquivos e no nível do SVM. Você pode criar outros usuários do sistema

de arquivos e do SVM, além de criar perfis adicionais do SVM para atender às necessidades da sua organização. Este capítulo explica os usuários e perfis do ONTAP, e apresenta procedimentos detalhados para criar usuários adicionais e perfis de SVM.

Perfis e usuários de administrador do sistema de arquivos

O usuário padrão do sistema de arquivos do ONTAP é `fsxadmin`, que tem o perfil `fsxadmin` atribuído a ele. Há dois perfis predefinidos que você pode atribuir aos usuários do sistema de arquivos, listadas a seguir:

- **`fsxadmin`**: os administradores com esse perfil têm direitos irrestritos no sistema ONTAP. Eles podem configurar todos os recursos do sistema de arquivos e do SVM disponíveis nos sistemas FSx de arquivos ONTAP.
- **`fsxadmin-readonly`**: os administradores com esse perfil podem ver tudo no nível do sistema de arquivos, mas não podem fazer nenhuma alteração.

  Esse perfil é adequado para uso com aplicações de monitoramento (p. ex., NetApp Harvest), porque ele tem acesso somente de leitura a todos os recursos disponíveis e suas propriedades, mas não pode fazer nenhuma alteração neles.

Você pode criar outros usuários do sistema de arquivos e atribuir a eles o perfil `fsxadmin` ou `fsxadmin-readonly`. Você não pode criar novos perfis nem modificar os perfis existentes. Para obter mais informações, consulte Criação de novos usuários do ONTAP para administração do sistema de arquivos e do SVM.

A tabela a seguir descreve o nível de acesso que os perfis de administrador do sistema de arquivos têm aos comandos e diretórios de comandos da API REST e da CLI do ONTAP.

Nome do perfil	Nível de acesso	Aos seguintes comandos ou diretórios de comandos
`fsxadmin`	tudo	Todos os diretórios de comando disponíveis no FSx for ONTAP
`fsxadmin-readonly`	tudo	`security login password`

Nome do perfil	Nível de acesso	Aos seguintes comandos ou diretórios de comandos
		Somente para gerenciar sua própria conta de usuário, senha local e informações de chave
	nenhuma	`security`
	somente leitura	Todos os outros diretórios de comando disponíveis no FSx for ONTAP

Perfis e usuários de administrador do SVM

Cada SVM tem um domínio de autenticação separado e pode ser gerenciado de modo independente por seus próprios administradores. Cada SVM em seu sistema de arquivos tem um usuário padrão chamado vsadmin, que tem o perfil `vsadmin` atribuído por padrão. Além do perfil `vsadmin`, há outros perfis predefinidos do SVM que fornecem permissões com escopo reduzido que você pode atribuir aos usuários do SVM. Você também pode criar perfis personalizados que forneçam o nível de controle de acesso adequado às necessidades da sua organização.

Os perfis predefinidos para administradores de SVM e seus recursos são os seguintes:

Nome do perfil	Capacidades
`vsadmin`	• Gerenciar sua conta de usuário, senha local e informações importantes • Gerenciar volumes, exceto movimentações de volume • Gerenciar cotas, qtrees, cópias de snapshots e arquivos • Gerenciar LUNs • Execute SnapLock operações, exceto para exclusão privilegiada

Nome do perfil	Capacidades
	• Configurar protocolos: NFS, SMB e iSCSI • Configurar serviços: DNS, LDAP e NIS • Monitorar trabalhos • Monitorar as conexões de rede e a interface de rede • Monitorar a integridade da SVM
`vsadmin-volume`	• Gerenciar sua conta de usuário, senha local e informações importantes • Gerenciar volumes, incluindo movimentos de volume • Gerenciar cotas, qtrees, cópias de snapshots e arquivos • Gerenciar LUNs • Configurar protocolos: NFS, SMB e iSCSI • Configurar serviços: DNS, LDAP e NIS • Monitorar a interface de rede. • Monitorar a integridade da SVM
`vsadmin-protocol`	• Gerenciar sua conta de usuário, senha local e informações importantes • Gerenciar LUNs • Configurar protocolos: NFS, SMB e iSCSI • Configurar serviços: DNS, LDAP e NIS • Monitorar a interface de rede. • Monitorar a integridade da SVM

Nome do perfil	Capacidades
`vsadmin-backup`	• Gerenciar sua conta de usuário, senha local e informações importantes • Gerenciar operações NDMP • Tornar um volume restaurado em leitura/gravação • Gerencie SnapMirror relacionamentos e cópias de instantâneos • Visualizar volumes e informações de rede
`vsadmin-snaplock`	• Gerenciar sua conta de usuário, senha local e informações importantes • Gerenciar volumes, exceto movimentações de volume • Gerenciar cotas, qtrees, cópias de snapshots e arquivos • Execute SnapLock operações, incluindo exclusão privilegiada • Configurar protocolos: NFS e SMB • Configurar serviços: DNS, LDAP e NIS • Monitorar trabalhos • Monitorar as conexões de rede e a interface de rede
`vsadmin-readonly`	• Gerenciar sua conta de usuário, senha local e informações importantes • Monitorar a integridade da SVM • Monitorar a interface de rede. • Visualize volumes e LUNs • Visualizar serviços e protocolos

Para obter mais informações sobre como criar um novo perfil de SVM, consulte Criação de perfis de SVM.

Como usar o Active Directory para autenticar usuários do ONTAP

Você pode autenticar o acesso dos usuários do domínio Windows Active Directory a um FSx sistema de arquivos ONTAP e SVM. Você deve executar as seguintes tarefas antes que as contas do Active Directory possam acessar seu sistema de arquivos:

- Você precisa configurar o acesso do controlador de domínio do Active Directory para o SVM.

  O SVM que você usa para configurar como gateway ou túnel para acesso ao controlador de domínio do Active Directory deve ter o CIFS habilitado, estar associado a um Active Directory ou ambos. Se você não estiver habilitando o CIFS e somente unindo a SVM do túnel a um Active Directory, certifique-se de que a SVM esteja associada ao Active Directory. Para obter mais informações, consulte Como funciona SVMs a adesão ao Microsoft Active Directory.
- Você precisa habilitar uma conta de usuário de domínio do Active Directory para acessar o sistema de arquivos.

  Você pode usar a autenticação por senha ou a autenticação de chave pública SSH para usuários de domínio do Windows que acessam a API REST ou a CLI do ONTAP.

Para ver os procedimentos que descrevem como configurar a autenticação do Active Directory para administradores de sistemas de arquivos e SVM, consulte Configuração da autenticação do Active Directory para usuários do ONTAP.

Criação de novos usuários do ONTAP para administração do sistema de arquivos e do SVM

Cada usuário do ONTAP está associado a uma SVM ou ao sistema de arquivos. Os usuários do sistema de arquivos com o perfil `fsxadmin` podem criar novos perfis e usuários do SVM usando o comando `security login create` da CLI do ONTAP.

O comando `security login create` cria um método de login para o utilitário de gerenciamento. Um método de login consiste em um nome de usuário, uma aplicação (método de acesso) e um método de autenticação. Um nome de usuário pode ser associado a várias aplicações. Opcionalmente, ele pode incluir um nome de perfil de controle de acesso. Se um nome de grupo do Active Directory, LDAP ou NIS for usado, o método de login concederá acesso aos usuários

pertencentes ao grupo especificado. Se o usuário integrar vários grupos provisionados na tabela de login de segurança, ele terá acesso a uma lista combinada dos comandos autorizados para cada grupo.

Para obter informações que descrevem como criar um novo usuário do ONTAP, consulte Criação de usuários do ONTAP.

Tópicos

- Criação de usuários do ONTAP
- Criação de perfis de SVM
- Configuração da autenticação do Active Directory para usuários do ONTAP
- Como configurar a autenticação de chave pública
- Atualização dos requisitos de senha para perfis de sistema de arquivos e SVM
- Falha na atualização da senha da conta fsxadmin

Criação de usuários do ONTAP

Criar um novo usuário da SVM ou do sistema de arquivos (CLI do ONTAP)

Somente usuários do sistema de arquivos com o perfil `fsxadmin` podem criar novos usuários da SVM e do sistema de arquivos.

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. Use o comando `security login create` ONTAP CLI para criar uma nova conta de usuário em seu FSx sistema de arquivos ONTAP ou SVM.

   Para definir as seguintes propriedades obrigatórias, insira seus dados nos espaços reservados no exemplo:

- `-vserver`: especifica o nome da SVM na qual você deseja criar o novo perfil ou usuário da SVM. Se você estiver criando um perfil ou usuário do sistema de arquivos, não especifique uma SVM.
- `-user-or-group-name`: especifica o nome de usuário ou nome do grupo do Active Directory do método de login. O nome do grupo do Active Directory só pode ser especificado com o método de autenticação `domain` e as aplicações `ontapi` e `ssh`.
- `-application`: especifica a aplicação do método de login. Os valores possíveis incluem http, ontapi e ssh.
- `-authentication-method`: especifica o método de autenticação para login. Os valores possíveis incluem o seguinte:
  - domain: use para autenticação do Active Directory.
  - password: use para autenticação por senha.
  - publickey: use para autenticação de chave pública.
- `-role`: especifica o nome do perfil de controle de acesso para o método de login. No nível do sistema de arquivos, o único perfilo que pode ser especificada é `fsxadmin`.

(Opcional) Também é possível usar um ou mais dos seguintes parâmetros com o comando:

- `[-comment]`: use para incluir uma anotação ou comentário à conta do usuário. Por exemplo, .**`Guest account`** O tamanho máximo é 128 caracteres.
- `[-second-authentication-method {none|publickey|password|nsswitch}]`: especifica o método de autenticação de segundo fator. É possível especificar os seguintes métodos:
  - password: use para autenticação por senha.
  - publickey: use para autenticação de chave pública.
  - nsswitch: use para autenticação NIS ou LDAP.
  - none: o valor padrão, se você não especificar nenhum.

```
Fsx0123456::> security login create -vserver vserver_name -user-or-group-
name user_or_group_name -application login_application -authentication-
method auth_method -role role_or_account_name
```

O comando a seguir cria um novo usuário `new_fsxadmin` do sistema de arquivos com o perfil `fsxadmin-readonly` atribuído, usando SSH com uma senha para fazer login. Quando solicitado, forneça uma senha para o usuário.

```
Fsx0123456::> security login create -user-or-group-name new_fsxadmin -application
 ssh -authentication-method password -role fsxadmin-readonly

Please enter a password for user 'new_fsxadmin':
Please enter it again:

Fsx0123456::>
```

3. O comando a seguir cria um novo usuário `new_vsadmin` da SVM no `fsx` da SVM com o perfil `vsadmin_readonly`, configurado para usar SSH com uma senha para fazer login. Quando solicitado, forneça uma senha para o usuário.

```
Fsx0123456::> security login create -vserver fsx  -user-or-group-name new_vsadmin -
application ssh -authentication-method password -role vsadmin-readonly

Please enter a password for user 'new_vsadmin':
Please enter it again:

Fsx0123456::>
```

4. O comando a seguir cria um novo usuário do sistema de arquivos somente para leitura `harvest2-user` que deve ser usado pelo aplicativo NetApp Harvest para coletar métricas de desempenho e capacidade. Para obter mais informações, consulte Monitoramento FSx de sistemas de arquivos ONTAP usando Harvest e Grafana.

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application
 ssh -role fsxadmin-readonly -authentication-method password
```

Visualizar informações de todos os usuários da SVM e do sistema de arquivos

- Use o comando a seguir para visualizar todas as informações de login do seu sistema de arquivos SVMs e.

```
Fsx0123456::> security login show
```

```
Vserver: Fsx0123456
                                                                 Second
User/Group                 Authentication                 Acct   Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------ --------------
autosupport    console     password      autosupport      no     none
fsxadmin       http        password      fsxadmin         no     none
fsxadmin       ontapi      password      fsxadmin         no     none
fsxadmin       ssh         password      fsxadmin         no     none
fsxadmin       ssh         publickey     fsxadmin         -      none
new_fsxadmin   ssh         password      fsxadmin-readonly
                                                        no     none

Vserver: fsx
                                                                 Second
User/Group                 Authentication                 Acct   Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------ --------------
new_vsadmin    ssh         password      vsadmin-readonly no     none
vsadmin        http        password      vsadmin          yes    none
vsadmin        ontapi      password      vsadmin          yes    none
vsadmin        ssh         password      vsadmin          yes    none
10 entries were displayed.

Fsx0123456::>
```

Criação de perfis de SVM

Cada SVM que você cria tem um administrador de SVM padrão atribuído ao perfil `vsadmin` predefinido. Além do conjunto de perfis de SVM predefinidos, você pode criar novos perfis de SVM. Se você precisar criar novos perfis para sua SVM, use o comando `security login role create` da CLI do ONTAP. Esse comando está disponível para administradores de sistemas de arquivos com o perfil `fsxadmin`.

Para criar um novo perfil de SVM (CLI do ONTAP)

1. Você pode criar um novo perfil do SVM usando o comando `security login role create` da ONTAP CLI:

```
Fsx0123456::> security login role create -vserver vs1.example.com -role vol_role -
cmddirname volume
```

2. Especifique os seguintes parâmetros obrigatórios no comando:

   - `-vserver`: o nome da SVM.
   - `-role`: o nome do perfil.
   - `-cmddirname`: o comando ou diretório de comando ao qual o perfil fornece acesso. Coloque entre aspas duplas os nomes dos subdiretórios de comandos. Por exemplo, ."`volume snapshot`" Digite `DEFAULT` para especificar todos os diretórios de comando.

3. (Opcional) Você também pode adicionar qualquer um dos seguintes parâmetros ao comando:

   - `-vserver`: o nome da SVM que está associada ao perfil.
   - `-access`: o nível de acesso do perfil. Para diretórios de comandos, isso inclui:
     - `none`: nega o acesso aos comandos do diretório. Este é o valor padrão dos perfis personalizados.
     - `readonly`: concede acesso aos comandos show no diretório de comandos e nos subdiretórios.
     - `all`: concede acesso a todos os comandos no diretório de comandos e nos subdiretórios. Para conceder ou negar acesso aos comandos intrínsecos, especifique o diretório de comandos.

     Para comandos não intrínsecos (comandos que não terminam com `create`, `modify`, `delete` ou `show`):

     - `none`: nega o acesso aos comandos do diretório. Este é o valor padrão dos perfis personalizados.
     - `readonly`: não aplicável. Não use:
     - `all`: concede acesso ao comando.
   - `-query`: o objeto de consulta usado para filtrar o nível de acesso, que é especificado na forma de opção válida para o comando ou para um comando no diretório de comandos. Coloque entre aspas duplas o objeto de consulta.

4. Execute o comando `security login role create`.

O comando a seguir cria um perfil de controle de acesso chamado “admin” para o Vserver vs1.example.com. O perfil tem acesso completo ao comando “volume”, mas somente dentro do agregado “aggr0”.

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-
aggr aggr0" -access all -vserver vs1.example.com
```

Configuração da autenticação do Active Directory para usuários do ONTAP

Use a CLI do ONTAP para configurar o uso da autenticação do Active Directory para usuários de SVM e do sistema de arquivos do ONTAP.

Para usar os comandos neste procedimento, é necessário ser um administrador do sistema de arquivos com o perfil `fsxadmin`.

Configurar a autenticação do Active Directory para usuários do ONTAP (CLI do ONTAP)

Os comandos desse procedimento estão disponíveis para usuários do sistema de arquivos com o perfil `fsxadmin`.

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.
2. Use o comando `security login domain-tunnel create` conforme apresentado para estabelecer um túnel de domínio para autenticar usuários do Active Directory do Windows. *`svm_name`*Substitua pelo nome do SVM que você está usando para o túnel de domínio.

   ```
   FsxId0123456::> security login domain-tunnel create -vserver svm_name
   ```
3. Use o comando `security login create` para criar contas de usuário de domínio do Active Directory que vão acessar o sistema de arquivos.

   Especifique os seguintes parâmetros obrigatórios no comando:

- `-vserver`: o nome do SVM configurado com o CIFS e associado ao seu Active Directory. Ele será usado como um túnel para autenticar os usuários do domínio do Active Directory no sistema de arquivos para o qual o novo perfil ou usuário será criado.
- `-user-or-group-name`: o nome de usuário ou nome do grupo do Active Directory do método de login. O nome do grupo do Active Directory só pode ser especificado com o método de autenticação `domain` e as aplicações `ontapi` e `ssh`.
- `-application`: a aplicação do método de login. Os valores possíveis incluem http, ontapi e ssh.
- `-authentication-method`: o método de autenticação usado para login. Os valores possíveis incluem o seguinte:
  - domain: para autenticação do Active Directory.
  - password: para autenticação por senha.
  - publickey: para autenticação de chave pública.
- `-role`: o nome do perfil de controle de acesso para o método de login. No nível do sistema de arquivos, o único perfilo que pode ser especificada é `-role fsxadmin`.

O exemplo a seguir cria uma conta de usuário `CORP\Admin` de domínio do Active Directory para o sistema de arquivos `filesystem1`.

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
application ssh -authmethod domain -role fsxadmin
```

O exemplo a seguir cria a conta de usuário `CORP\Admin` com autenticação de chave pública.

```
FsxId0123456ab::> security login create -user-or-group-name "CORP\Admin" -
application ssh -authentication-method publickey -role fsxadmin
Warning: To use public-key authentication, you must create a public key for user
 "CORP\Admin".
```

Crie uma chave pública para o usuário `CORP\Admin` com o comando a seguir:

```
FsxId0123456ab::> security login publickey create -username "CORP
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=
 cwaltham@b0be837a91bf.ant.amazon.com"
```

Para fazer login no sistema de arquivos usando SSH com credenciais do Active Directory

- O exemplo a seguir demonstra como efetuar SSH no sistema de arquivos com as credenciais do Active Directory, se você escolher `ssh` para o tipo `-application`. O `username` está no formato `"domain-name\user-name"`, que é o nome do domínio e o nome de usuário que você forneceu ao criar a conta, separados por uma barra invertida e entre aspas.

  ```
  Fsx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
  ```

  Quando solicitado a digitar uma senha, use a senha do usuário do Active Directory.

Como configurar a autenticação de chave pública

Para habilitar a autenticação de chave pública SSH, você deve primeiro gerar uma chave SSH e associá-la a uma conta de administrador usando o comando `security login publickey create`. Isso permite que a conta acesse a SVM. O comando `security login publickey create` aceita os seguintes parâmetros:

Parameter	Descrição
`-vserver` (Opcional)	O nome da SVM que a conta acessa. Se você estiver configurando a autenticação de chave pública SSH para usuários do sistema de arquivos, não inclua `-versver`.
`-username`	O nome de usuário da conta. O valor padrão, `admin`, é o nome padrão do administrador do cluster.
`-index`	O número de índice da chave pública. O valor padrão será 0 se a chave for a primeira criada para a conta. Caso contrário, o valor padrão será um a mais do que o maior número de índice existente para a conta.
`-publickey`	A chave pública OpenSSH. Coloque a chave entre aspas duplas.

Parameter	Descrição
`-role`	O perfil de controle de acesso atribuído à conta.
`-comment` (Opcional)	Texto descritivo da chave pública. Coloque o texto entre aspas duplas.

O exemplo a seguir associa uma chave pública à conta de administrador `svmadmin` da SVM `svm01`. A chave pública recebe o número de índice 5.

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J/
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

> **Important**
>
> Você deve ser administrador da SVM ou do sistema de arquivos para executar essa tarefa.

Atualização dos requisitos de senha para perfis de sistema de arquivos e SVM

Você pode atualizar os requisitos de senha para um perfil de SVM ou sistema de arquivos usando o comando `security login role config modify` da CLI do ONTAP. Esse comando está disponível somente para contas de administrador do sistema de arquivos com o perfil `fsxadmin`. Ao modificar os requisitos de senha, o sistema avisará se houver algum usuário existente com esse perfil que seja afetado pela alteração.

O exemplo a seguir modifica o requisito de tamanho mínimo da senha para 12 caracteres para usuários com o perfil `vsadmin-readonly` na SVM `fsx`. Neste exemplo, há usuários existentes com esse perfil.

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

O sistema exibe o seguinte aviso devido aos usuários existentes:

```
Warning: User accounts with this role exist. Modifications to the username/password
 restrictions on this role could result in non-compliant user
         accounts.
Do you want to continue? {y|n}:

FsxId0123456::>
```

Falha na atualização da senha da conta `fsxadmin`

Ao atualizar a senha do usuário `fsxadmin`, você poderá receber um erro se ela não atender aos requisitos de senha definidos no sistema de arquivos. É possível visualizar os requisitos de senha usando o comando `security login role config show` na CLI ou na API REST do ONTAP.

Visualizar os requisitos de senha para um perfil de sistema de arquivos ou SVM

1. Para acessar a ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o comando a seguir. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

2. O comando `security login role config show` retorna os requisitos de senha para um perfil de sistema de arquivos ou SVM.

   ```
   FsxId0123456::> security login role config show -role fsxadmin -
   fields password_requirement_fields
   ```

   Para o parâmetro `-fields`, especifique uma ou todas das seguintes opções:

   - `passwd-minlength`: o tamanho mínimo da senha.
   - `passwd-min-special-chars`: o número mínimo de caracteres especiais na senha.
   - `passwd-min-lowercase-chars`: o número mínimo de letras minúsculas na senha.
   - `passwd-min-uppercase-chars`: o número mínimo de letras maiúsculas na senha.

- `passwd-min-digits`: o número mínimo de dígitos na senha.
- `passwd-alphanum`: informações sobre inclusão ou exclusão de caracteres alfanuméricos.
- `passwd-expiry-time`: a data de validade da senha.
- `passwd-expiry-warn-time`: o tempo do aviso de validade da senha.

3. Execute o comando a seguir para visualizar todos os requisitos de senha:

```
FsxId0123456::> security login role config show -role fsxadmin -fields passwd-
minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
uppercase-chars

vserver                role     passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
---------------------- -------- ---------------- ---------------
 ------------------------ ------------------ --------------------------
 -------------------------- ----------------- ----------------------
FsxId0123456           fsxadmin 3                enabled         0
       unlimited          0                        0                        0
               unlimited
```

Cotas

A seguir, você pode descobrir mais sobre cotas ao trabalhar com a Amazon FSx para NetApp ONTAP.

Tópicos

- Cotas que podem ser aumentadas
- Cotas de recursos para cada sistema de arquivos

Cotas que podem ser aumentadas

A seguir estão as cotas da Amazon FSx para NetApp ONTAP para cada uma Conta da AWS que você pode aumentar. Região da AWS

Recurso	Padrão	Descrição
ONTAP sistemas de arquivos	100	O número máximo de sistemas de arquivos Amazon FSx for NetApp ONTAP que você pode criar nessa conta.
ONTAP Capacidade de armazenamento SSD	524.288	A quantidade máxima de capacidade de armazenam ento SSD (em GiB) para todos os sistemas de arquivos FSx Amazon NetApp for ONTAP que você pode ter nessa conta.
ONTAP Capacidade de throughput	10,240	A quantidade máxima de capacidade de transferência (em MBps) para todos os sistemas de arquivos Amazon FSx for NetApp ONTAP que você pode ter nessa conta.

Recurso	Padrão	Descrição
ONTAP IOPS SSD	1.000.000	A quantidade máxima de SSD IOPS para todos os sistemas de arquivos Amazon FSx for NetApp ONTAP que você pode ter nessa conta.
ONTAP backups	10.000	O número máximo de backups de volume iniciados pelo usuário para todos os sistemas de arquivos Amazon FSx for NetApp ONTAP que você pode ter em um. Conta da AWS

Para solicitar um aumento da cota

1. Abra a página AWS Support, faça login se necessário e escolha Create case (Criar caso).
2. Em Criar caso, escolha Suporte para conta e faturamento.
3. No painel Detalhes do caso, faça as seguintes entradas:
   - Em Tipo, escolha Conta.
   - Em Categoria, escolha Outros problemas de conta.
   - Em Assunto, insira **`Amazon FSx for NetApp ONTAP service limit increase request`**.
   - Forneça uma Descrição detalhada de sua solicitação, incluindo:
     - A FSx cota que você deseja aumentar e o valor para o qual deseja aumentar, se conhecido.
     - O motivo de estar buscando o aumento da cota.
     - O ID do sistema de arquivos e a região de cada sistema de arquivos para o qual você está solicitando um aumento.
4. Forneça suas Opções de contato preferenciais e escolha Enviar.

Cotas de recursos para cada sistema de arquivos

A tabela a seguir lista as cotas na Amazon FSx para recursos NetApp ONTAP para cada sistema de arquivos em um. Região da AWS

Recurso	Limite por sistema de arquivos
Capacidade mínima de armazenamento SSD	1.024 GiB por par de alta disponibi lidade (HA)
Capacidade máxima de armazenamento SSD	• Sistemas de arquivos Single-AZ de segunda geração: 512 TiB por par de HA, até 1 PiB • Sistemas de arquivos Multi-AZ de segunda geração: 512 TiB • Sistemas de arquivos de primeira geração: 192 TiB
IOPS de SSD máxima	Sistemas de arquivos de segunda geração: • 200.000 por par de HA (até 12 pares) para Single-AZ • Total de 200.000 para Multi-AZ Sistemas de arquivos de primeira geração: • 160.000 nas regiões Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda) • 80.000 em todos os outros Regiões da AWS lugares onde FSx o ONTAP está disponível

Recurso	Limite por sistema de arquivos
Capacidade de throughput mínima	• Sistemas de arquivos de segunda geração (1 par HA): 384 MBps • Sistemas de arquivos de segunda geração (2 ou mais pares de HA): 1.536 MBps por par de HA • Sistemas de arquivos de primeira geração: 128 MBps
Capacidade de throughput máxima	Sistemas de arquivos de segunda geração: • 73.728 MBps 1 para Single-AZ • 6.144 MBps para Multi-AZ Sistemas de arquivos de primeira geração: • 4.096 MBps [2] na Região Leste dos EUA (Ohio), Região Leste dos EUA (Norte da Virgínia), Região Oeste dos EUA (Oregon) e Europa (Irlanda) • 2.048 MBps em todos os outros Regiões da AWS lugares onde o FSx ONTAP está disponível
Número máximo de volumes	• Sistemas de arquivos de segunda geração (1 par de HA): 500 • Sistemas de arquivos de segunda geração (2 ou mais pares de HA): 1.000 • Sistemas de arquivos de primeira geração: 500

Recurso	Limite por sistema de arquivos
Número máximo de snapshots	1.023 por volume[3]
Número máximo de backups	4.091 por volume[4]

Recurso	Limite por sistema de arquivos
Número máximo de SVMs	Sistemas de arquivos de segunda geração com um par de HA: • 6 (384 MBps da capacidade de produção) • 6 (768 MBps da capacidade de processamento) • 14 (1.536 de capacidade MBps de processamento) • 14 (3.072 MBps de capacidade de processamento) • 24 (6.144 MBps da capacidade de produção) Sistemas de arquivos de segunda geração com 2 a 12 pares de HA: • 5 Sistemas de arquivos de primeira geração: • 6 (128 capacidade MBps de processamento) • 6 (capacidade de MBps processamento de 256) • 14 (capacidade de MBps processamento de 512) • 14 (capacidade de MBps processamento de 1.024) • 24 (capacidade de MBps processamento de 2.048)

Recurso	Limite por sistema de arquivos
	• 24 (capacidade de MBps processamento de 4.096)
Número máximo de tags	50
Período máximo de retenção para backups automatizados	90 dias
Período máximo de retenção para backups iniciados pelo usuário	Sem limite de retenção
Número máximo de rotas suportadas por sistema de arquivos	50 [5]
Número máximo de conexões de cliente por servidor de arquivos [6]	100.000

Note

[1] Em um sistema de arquivos Single-AZ de segunda geração com 12 pares de HA (6.144 MBps por par de HA). Para obter mais informações, consulte Gerenciar pares de alta disponibilidade (HA).

[2] Para provisionar 4% GBps da capacidade de taxa de transferência, seu FSx sistema de arquivos de primeira geração do ONTAP requer uma configuração de SSD IOPS máxima (160.000) e um mínimo de 5.120 GiB de capacidade de armazenamento SSD em um ambiente compatível. Região da AWS Para obter mais informações sobre quais Regiões da AWS suportam 4.096 MBps da capacidade de taxa de transferência, consulte. Impacto da capacidade de throughput na performance

[3] Você pode armazenar até 1.023 snapshots por volume em qualquer ponto no tempo. Após atingir esse limite, você deverá excluir um snapshot existente antes que um novo snapshot do volume possa ser criado.

[4] Você pode armazenar até 4.091 backups por volume em qualquer ponto no tempo. Após atingir esse limite, você deverá excluir um backup existente antes que o sistema possa criar um novo backup do volume.

[5] Você pode configurar até 50 rotas por sistema de arquivos a qualquer momento. Após atingir esse limite, você deverá excluir uma rota existente antes que o sistema

possa configurar uma nova rota. O número de rotas que seu sistema de arquivos tem é determinado pelo número de SVMs rotas e pelo número de tabelas de rotas associadas a ele. Você pode determinar o número existente de rotas para um sistema de arquivos usando a seguinte equação: (1 + número de SVMs no sistema de arquivos) * (tabelas de rotas associadas ao sistema de arquivos).

[6] Uma conexão de cliente é definida como uma única conexão TCP com um determinado servidor de arquivos. Há um servidor de arquivos ativo por par de HA em um sistema de arquivos. Um cliente pode ter várias conexões TCP com um servidor de arquivos. Por exemplo, se um cliente estiver usando vários caminhos.

Solução de problemas da Amazon FSx para NetApp ONTAP

Use as seções a seguir para ajudar a solucionar problemas nos sistemas FSx de arquivos ONTAP.

Tópicos

- Seu sistema de arquivos está em um MISCONFIGURED estado
- Não é possível acessar o sistema de arquivos
- Sua máquina virtual de armazenamento (SVM) está em um estado MISCONFIGURED
- Não é possível associar uma máquina virtual de armazenamento (SVM) ao Active Directory
- Não é possível excluir um volume ou uma máquina virtual de armazenamento
- Seu volume está em um MISCONFIGURED estado
- Seu volume tem capacidade de armazenamento insuficiente
- Seus backups falham devido à capacidade insuficiente de volume
- Corrigir problemas de rede

Seu sistema de arquivos está em um **`MISCONFIGURED`** estado

Há várias possíveis causas para que um sistema de arquivos esteja no estado `MISCONFIGURED`, cada uma com sua própria solução, conforme apresentado a seguir.

Tópicos

- A conta do proprietário da VPC desabilitou o compartilhamento de VPC Multi-AZ
- Você não pode criar uma nova SVM em um sistema de arquivos Multi-AZ
- O nível de armazenamento SSD do seu sistema de arquivos está mais de 90% cheio

A conta do proprietário da VPC desabilitou o compartilhamento de VPC Multi-AZ

Os sistemas de arquivos Multi-AZ criados por um participante Conta da AWS em uma sub-rede VPC compartilhada entrarão em `MISCONFIGURED` um estado por um dos seguintes motivos:

- A conta do proprietário que compartilhou a sub-rede VPC desativou o suporte ao compartilhamento de VPC Multi-AZ para sistemas de arquivos ONTAP. FSx

- A conta do proprietário parou de compartilhar a sub-rede VPC.

Se a conta do proprietário tiver parado de compartilhar a sub-rede VPC, você verá a seguinte mensagem no console desse sistema de arquivos:

```
The vpc ID vpc-012345abcde does not exist
```

Para resolver o problema, você precisa entrar em contato com a conta do proprietário que compartilhou a sub-rede VPC com você. Para obter mais informações, consulte Criação FSx para sistemas de arquivos ONTAP em sub-redes compartilhadas.

Você não pode criar uma nova SVM em um sistema de arquivos Multi-AZ

Para sistemas de arquivos Multi-AZ criados por um participante Conta da AWS em uma VPC compartilhada, você não conseguirá criar uma nova SVM por um dos seguintes motivos:

- A conta do proprietário que compartilhou a sub-rede VPC desativou o suporte ao compartilhamento de VPC Multi-AZ para sistemas de arquivos ONTAP. FSx
- A conta do proprietário parou de compartilhar a sub-rede VPC.

Para resolver o problema, você precisa entrar em contato com a conta do proprietário que compartilhou a sub-rede VPC com você. Para obter mais informações, consulte Criação FSx para sistemas de arquivos ONTAP em sub-redes compartilhadas.

O nível de armazenamento SSD do seu sistema de arquivos está mais de 90% cheio

O nível de armazenamento SSD do seu sistema de arquivos Single-AZ ou Multi-AZ está atualmente mais de 90% cheio. Recomendamos que você não ultrapasse continuamente 80% de utilização do nível de armazenamento SSD. Se você não liberar espaço na camada de armazenamento SSD antes da próxima janela de manutenção do sistema de arquivos, o FSx for ONTAP reduzirá temporariamente a taxa de transferência do sistema de arquivos durante a operação de patch. Isso é feito para garantir que os processos de manutenção em segundo plano possam ser concluídos dentro de um período de tempo razoável. Para evitar isso, reduza a utilização do seu nível de armazenamento SSD para menos de 90%. Você pode reduzir a utilização do SSD de várias maneiras, incluindo:

- Aumentando a capacidade de armazenamento SSD do seu sistema de arquivos.
- Excluindo dados desnecessários.
- Excluindo instantâneos de volume desnecessários.

Para obter mais informações, consulte Como gerenciar a capacidade de armazenamento.

Não é possível acessar o sistema de arquivos

Esta seção descreve problemas e soluções relacionados à impossibilidade de acessar seu sistema de arquivos.

Tópicos

- Seu sistema de arquivos Multi-AZ não tem tags de tabela de rotas
- Seu sistema de arquivos tem mais de 50 rotas
- Seu sistema de arquivos não tem rotas para um ou mais servidores de arquivos
- A interface de rede elástica do sistema de arquivos foi modificada ou excluída
- O endereço IP elástico anexado à interface de rede elástica do sistema de arquivos foi excluído
- O grupo de segurança da VPC do sistema de arquivos não tem as regras de entrada necessárias
- O grupo de segurança da VPC da instância de computação não tem as regras de saída necessárias
- A sub-rede da instância de computação não usa nenhuma das tabelas de rotas associadas ao seu sistema de arquivos
- A Amazon não FSx pode atualizar a tabela de rotas para sistemas de arquivos Multi-AZ criados usando AWS CloudFormation
- Não é possível acessar um sistema de arquivos por meio do iSCSI de um cliente em outra VPC
- A conta proprietária parou de compartilhar a sub-rede VPC
- Não é possível acessar um sistema de arquivos por meio de NFS, SMB, CLI do ONTAP ou API REST do ONTAP de um cliente em outra VPC ou on-premises

Seu sistema de arquivos Multi-AZ não tem tags de tabela de rotas

A Amazon FSx gerencia tabelas de rotas de VPC para sistemas de arquivos Multi-AZ usando autenticação baseada em tags. No momento, uma ou mais tabelas de rotas associadas ao seu

sistema de arquivos não têm essas tags de tabela de rotas. Essas tabelas de rotas serão marcadas com `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Se você não adicionar manualmente essas tags antes da próxima janela de manutenção, todos os clientes em sub-redes associadas às tabelas de rotas que não tenham as tags perderão temporariamente o acesso ao sistema de arquivos durante a operação de patch. Para evitar isso, adicione manualmente as tags da tabela de rotas ausentes.

Para obter mais informações, consulte Atualizar sistemas de arquivos.

Seu sistema de arquivos tem mais de 50 rotas

Atualmente, seu sistema de arquivos tem mais de 50 rotas associadas a ele. Se você não remover algumas dessas rotas antes da próxima janela de manutenção programada do sistema de arquivos, o processo de failover poderá demorar mais do que o normal. Para evitar isso, reduza o número de rotas para menos de 50. A seguir estão as etapas que você pode seguir para reduzir o número de rotas associadas ao seu sistema de arquivos:

- Excluindo qualquer rota em excesso
- Reduzindo o número de SVMs associados ao sistema de arquivos
- Reduzindo o número de tabelas de rotas associadas ao sistema de arquivos

Para obter mais informações, consulte Atualizar sistemas de arquivos e Excluir máquinas virtuais de armazenamento (SVM).

Seu sistema de arquivos não tem rotas para um ou mais servidores de arquivos

No momento, seu sistema de arquivos não tem rotas para um ou mais servidores de arquivos, e as tabelas de rotas existentes não têm espaço suficiente para adicionar novas entradas na tabela de rotas. Se você não adicionar as rotas ausentes antes da próxima janela de manutenção programada do sistema de arquivos, todos os clientes conectados serão desconectados durante a operação de correção. Para evitar isso, adicione as rotas que faltam.

Para obter mais informações, consulte Atualizar sistemas de arquivos e Cotas.

A interface de rede elástica do sistema de arquivos foi modificada ou excluída

Você não deve modificar nem excluir nenhuma das interfaces de rede elástica do sistema de arquivos. Modificar ou excluir uma interface de rede pode causar uma perda permanente de conexão entre a nuvem privada virtual (VPC) e o sistema de arquivos. Crie um novo sistema de arquivos e não modifique nem exclua a interface de FSx rede da Amazon. Para obter mais informações, consulte Controle de acesso ao sistema de arquivos com a Amazon VPC.

O endereço IP elástico anexado à interface de rede elástica do sistema de arquivos foi excluído

A Amazon FSx não oferece suporte ao acesso a sistemas de arquivos da Internet pública. A Amazon separa FSx automaticamente qualquer endereço IP elástico, que é um endereço IP público acessível pela Internet e anexado à interface de rede elástica de um sistema de arquivos. Para obter mais informações, consulte Clientes compatíveis.

O grupo de segurança da VPC do sistema de arquivos não tem as regras de entrada necessárias

Analise as regras de entrada especificadas em Grupos de segurança da Amazon VPC e certifique-se de que o grupo de segurança associado ao seu sistema de arquivos tenha as regras de entrada correspondentes.

O grupo de segurança da VPC da instância de computação não tem as regras de saída necessárias

Analise as regras de saída especificadas em Grupos de segurança da Amazon VPC e certifique-se de que o grupo de segurança associado à sua instância de computação tenha as regras de saída correspondentes.

A sub-rede da instância de computação não usa nenhuma das tabelas de rotas associadas ao seu sistema de arquivos

FSx for ONTAP cria endpoints para acessar seu sistema de arquivos em uma tabela de rotas de VPC. Recomendamos que configure o sistema de arquivos para usar todas as tabelas de rotas da

VPC associadas às sub-redes nas quais seus clientes estão localizados. Por padrão, a Amazon FSx usa a tabela de rotas principal da sua VPC. Opcionalmente, você pode especificar uma ou mais tabelas de rotas para FSx a Amazon usar ao criar seu sistema de arquivos.

Se você consegue fazer ping no endpoint intercluster do sistema de arquivos, mas não no endpoint de gerenciamento do sistema de arquivos (consulte Recursos do sistema de arquivos para obter mais informações), é provável que seu cliente não esteja em uma sub-rede associada a uma das tabelas de rotas do sistema de arquivos. Para acessar seu sistema de arquivos, associe uma das tabelas de rotas do sistema de arquivos à sub-rede do seu cliente. Para obter informações sobre como atualizar tabelas de rotas da Amazon VPC do sistema de arquivos, consulte Atualizar sistemas de arquivos.

A Amazon não FSx pode atualizar a tabela de rotas para sistemas de arquivos Multi-AZ criados usando AWS CloudFormation

A Amazon FSx gerencia tabelas de rotas de VPC para sistemas de arquivos Multi-AZ usando autenticação baseada em tags. Essas tabelas de rotas serão marcadas com `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Ao criar ou atualizar FSx para sistemas de arquivos ONTAP Multi-AZ usando, AWS CloudFormation recomendamos que você adicione a `Key: AmazonFSx; Value: ManagedByAmazonFSx` tag manualmente.

Se você não conseguir acessar seu sistema de arquivos Multi-AZ, verifique se as tabelas de rotas da VPC associadas ao sistema de arquivos estão marcadas com `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Caso contrário, a Amazon FSx não poderá atualizar essas tabelas de rotas para rotear os endereços IP flutuantes das portas de gerenciamento e de dados para o servidor de arquivos ativo quando ocorrer um evento de failover. Para obter informações sobre como atualizar tabelas de rotas da Amazon VPC do sistema de arquivos, consulte Atualizar sistemas de arquivos.

Não é possível acessar um sistema de arquivos por meio do iSCSI de um cliente em outra VPC

Para acessar um sistema de arquivos por meio do protocolo Internet Small Computer Systems Interface (iSCSI) de um cliente em outra VPC, você pode configurar o emparelhamento da Amazon VPC ou o AWS Transit Gateway entre a VPC associada ao seu sistema de arquivos e a VPC na qual seu cliente reside. Para obter mais informações, consulte Criar e aceitar conexões de emparelhamento da VPC no guia da Amazon Virtual Private Cloud.

A conta proprietária parou de compartilhar a sub-rede VPC

Se você criou seu sistema de arquivos em uma sub-rede VPC que foi compartilhada com você, a conta proprietária pode ter parado de compartilhar a sub-rede VPC.

Se a conta do proprietário tiver parado de compartilhar a sub-rede VPC, você verá a seguinte mensagem no console desse sistema de arquivos:

```
The vpc ID vpc-012345abcde does not exist
```

Você precisará entrar em contato com a conta proprietária para que ela possa compartilhar novamente a sub-rede com você.

Não é possível acessar um sistema de arquivos por meio de NFS, SMB, CLI do ONTAP ou API REST do ONTAP de um cliente em outra VPC ou on-premises

Para acessar um sistema de arquivos via Network File System (NFS), Server Message Block (SMB) ou NetApp ONTAP CLI e REST API de um cliente em outra VPC ou no local, você deve configurar o roteamento usando AWS Transit Gateway entre a VPC associada ao seu sistema de arquivos e a rede na qual seu cliente reside. Para obter mais informações, consulte Acessando seus dados FSx do ONTAP.

Sua máquina virtual de armazenamento (SVM) está em um estado **`MISCONFIGURED`**

Há várias causas possíveis para uma máquina virtual de armazenamento entrar em um `MISCONFIGURED` estado, cada uma com sua própria resolução, conforme a seguir.

Seu SVM tem um volume off-line

Seu sistema de arquivos contém um volume que está em um estado off-line. Recomendamos que você mantenha os volumes on-line de forma contínua. Se você não colocar esse volume on-line antes da próxima janela de manutenção do seu sistema de arquivos, a Amazon o FSx colocará temporariamente on-line durante a operação de correção. Para evitar isso, conecte ou exclua o volume.

Para colocar um volume off-line novamente on-line, use o `volume online` ONTAP Comando CLI, conforme mostrado no exemplo a seguir. Se existir apenas um SVM (Vserver), você não precisará especificar o `-vserver` parâmetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Seu SVM tem um volume off-line com um iSCSI LUN ou um namespace / TCP NVMe

Seu sistema de arquivos contém um volume que está em um estado restrito. Recomendamos que você mantenha os volumes on-line de forma contínua. Se você não colocar esse volume on-line antes da próxima janela de manutenção do seu sistema de arquivos, a Amazon o FSx colocará temporariamente on-line durante a operação de correção. Para evitar isso, conecte ou exclua o volume.

Para colocar um volume off-line novamente on-line, use o `volume online` ONTAP Comando CLI, conforme mostrado no exemplo a seguir. Se existir apenas um SVM (Vserver), você não precisará especificar o `-vserver` parâmetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Não é possível associar uma máquina virtual de armazenamento (SVM) ao Active Directory

Se você não conseguir associar uma SVM a um Active Directory (AD), primeiro analise Como funciona SVMs a adesão ao Microsoft Active Directory. Problemas comuns que impedem uma SVM de se associar ao Active Directory estão listados nas seções a seguir, incluindo as mensagens de erro geradas para cada circunstância.

Tópicos

- O nome NetBIOS da SVM é igual ao nome NetBIOS do domínio inicial.
- A SVM já está associada a outro Active Directory

- A Amazon não FSx pode se conectar aos seus controladores de domínio do Active Directory porque o nome NetBIOS do SVM já está em uso
- A Amazon não FSx consegue se comunicar com seus controladores de domínio do Active Directory
- A Amazon não FSx consegue se conectar ao seu Active Directory devido a requisitos de porta ou permissões de conta de serviço não atendidos
- A Amazon não FSx pode se conectar aos seus controladores de domínio do Active Directory porque as credenciais da conta de serviço não são válidas
- A Amazon não FSx consegue se conectar aos seus controladores de domínio do Active Directory devido à insuficiência de credenciais da conta de serviço
- A Amazon não FSx consegue se comunicar com seus servidores DNS ou controladores de domínio do Active Directory
- A Amazon não FSx consegue se comunicar com seu Active Directory devido a um nome de domínio inválido do Active Directory.
- A conta de serviço não consegue acessar o grupo de administradores especificado na configuração do Active Directory da SVM
- A Amazon não FSx pode se conectar aos controladores de domínio do Active Directory porque a unidade organizacional especificada não existe ou não está acessível

O nome NetBIOS da SVM é igual ao nome NetBIOS do domínio inicial.

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

FSx A Amazon não consegue estabelecer uma conexão com seu Active Directory. Isso ocorre porque o nome do servidor especificado é o nome NetBIOS do domínio inicial. Para corrigir esse problema, escolha um nome NetBIOS para a sua SVM que seja diferente do nome NetBIOS do domínio inicial. Em seguida, tente associar novamente a SVM ao Active Directory.

Para resolver esse problema, siga o procedimento descrito em Ingressando SVMs no Active Directory usando a API AWS Management Console, AWS CLI e para tentar associar novamente a SVM ao AD. Certifique-se de usar um nome NetBIOS para a SVM que seja diferente do nome NetBIOS do domínio inicial do Active Directory.

A SVM já está associada a outro Active Directory

Ocorre uma falha ao associar uma SVM a um Active Directory com a seguinte mensagem de erro:

FSx A Amazon não consegue estabelecer uma conexão com seu Active Directory. Isso ocorre porque a SVM já está associada a um domínio. Para associar essa SVM a um domínio diferente, você pode usar a CLI do ONTAP ou a API REST para desassociá-la do Active Directory. Em seguida, tente associar novamente a SVM a um Active Directory diferente.

Para resolver o problema, faça o seguinte:

1. Use a CLI do NetApp ONTAP para desassociar o SVM do Active Directory atual. Para obter mais informações, consulte Desassocie um Active Directory do seu SVM usando a CLI do NetApp ONTAP.
2. Siga o procedimento descrito em Ingressando SVMs no Active Directory usando a API AWS Management Console, AWS CLI e para tentar associar novamente a SVM ao novo AD.

A Amazon não FSx pode se conectar aos seus controladores de domínio do Active Directory porque o nome NetBIOS do SVM já está em uso

Ocorre uma falha ao criar uma SVM associada ao AD autogerenciado com a seguinte mensagem de erro:

FSx A Amazon não consegue estabelecer uma conexão com seu Active Directory. Isso ocorre porque o nome NetBIOS (computador) especificado já está em uso no Active Directory. Para corrigir esse problema, escolha um nome NetBIOS para a SVM que não esteja em uso no Active Directory, especificando um NetBIOS (computador). Em seguida, tente associar novamente a SVM ao Active Directory.

Para resolver esse problema, siga o procedimento descrito em Ingressando SVMs no Active Directory usando a API AWS Management Console, AWS CLI e para tentar associar novamente a SVM ao AD. Certifique-se de usar um nome NetBIOS para a SVM que seja exclusivo e ainda não esteja em uso no Active Directory.

A Amazon não FSx consegue se comunicar com seus controladores de domínio do Active Directory

Ocorre uma falha ao associar uma SVM ao AD autogerenciado com a seguinte mensagem de erro:

A Amazon FSx não consegue se comunicar com seu Active Directory. Para corrigir esse problema, certifique-se de que o tráfego de rede seja permitido entre a Amazon FSx e seus controladores de domínio. Em seguida, tente associar novamente a SVM ao Active Directory.

Para resolver esse problema, faça o seguinte:

1. Analise os requisitos descritos em Requisitos de configuração de rede e faça as alterações necessárias para permitir a comunicação de rede entre a Amazon FSx e seu AD.
2. Quando a Amazon conseguir FSx se comunicar com seu AD, siga o procedimento descrito em Ingressando SVMs no Active Directory usando a API AWS Management Console, AWS CLI e e tente novamente unir seu SVM ao seu AD.

A Amazon não FSx consegue se conectar ao seu Active Directory devido a requisitos de porta ou permissões de conta de serviço não atendidos

Ocorre uma falha ao associar uma SVM ao AD autogerenciado com a seguinte mensagem de erro:

FSx A Amazon não consegue estabelecer uma conexão com seu Active Directory. Isso se deve ao fato de os requisitos de porta do Active Directory não serem atendidos ou a conta de serviço fornecida não ter permissões para associar a máquina virtual de armazenamento ao domínio com a unidade organizacional especificada. Para corrigir esse problema, atualize a configuração do Active Directory da sua máquina virtual de armazenamento depois de resolver quaisquer problemas de permissão com portas e contas de serviço, conforme recomendado no guia do FSx usuário da Amazon.

Para resolver esse problema, faça o seguinte:

1. Analise os requisitos descritos em Requisitos de configuração de rede e faça as alterações necessárias para atender aos requisitos de rede e garantir que as comunicações estejam habilitadas nas portas necessárias
2. Analise os requisitos da conta de serviço descritos em Requisitos de conta de serviço do Active Directory. Certifique-se de que a conta de serviço tenha as permissões delegadas necessárias para associar a SVM ao domínio do AD usando a unidade organizacional especificada.
3. Depois de fazer alterações nas permissões de porta ou na conta de serviço, siga o procedimento descrito em Ingressando SVMs no Active Directory usando a API AWS Management Console, AWS CLI e e tente associar novamente a SVM ao AD.

A Amazon não FSx pode se conectar aos seus controladores de domínio do Active Directory porque as credenciais da conta de serviço não são válidas

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

FSx A Amazon não consegue estabelecer uma conexão com seus controladores de domínio do Active Directory porque as credenciais da conta de serviço fornecidas são inválidas. Para corrigir esse problema, atualize a configuração do Active Directory da sua máquina virtual de armazenamento com uma conta de serviço válida.

Para resolver esse problema, use o procedimento descrito em Atualizando as configurações existentes do SVM Active Directory usando a API AWS Management Console, AWS CLI, e para atualizar as credenciais da conta de serviço da SVM. Ao inserir o nome de usuário da conta de serviço, inclua somente o nome do usuário (por exemplo, `ServiceAcct`) e não inclua nenhum prefixo de domínio (por exemplo, `corp.com\ServiceAcct`) ou sufixo de domínio (por exemplo, `ServiceAcct@corp.com`). Não use o nome distinto (DN) ao inserir o nome de usuário da conta de serviço (por exemplo, `CN=ServiceAcct,OU=example,DC=corp,DC=com`).

A Amazon não FSx consegue se conectar aos seus controladores de domínio do Active Directory devido à insuficiência de credenciais da conta de serviço

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

A Amazon FSx não consegue estabelecer uma conexão com seu (s) controlador (es) de domínio do Active Directory. Isso se deve a requisitos de porta não atendidos para o Active Directory ou à conta de serviço fornecida não ter permissão para unir a máquina virtual de armazenamento ao domínio com a unidade organizacional especificada.

Para resolver esse problema, certifique-se de ter delegado as permissões necessárias à conta de serviço fornecida. A conta de serviço deve ser capaz de criar e excluir objetos de computador na UO no domínio ao qual você está associando o sistema de arquivos. A conta de serviço também precisa, no mínimo, ter permissões para fazer o seguinte:

- Redefinir senhas

- Restringir contas de ler e gravar dados
- Capacidade validada para gravar no nome do host DNS
- Capacidade validada para gravar no nome da entidade principal de serviço
- Capacidade para criar e excluir objetos de computador
- Capacidade validada para ler e gravar restrições de conta

Para obter mais informações sobre como criar uma conta de serviço com as permissões corretas, consulte Requisitos de conta de serviço do Active Directory e Delegando permissões à sua conta de FSx serviço da Amazon.

A Amazon não FSx consegue se comunicar com seus servidores DNS ou controladores de domínio do Active Directory

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

A Amazon FSx não consegue se comunicar com seu Active Directory. Isso ocorre porque a Amazon não FSx consegue acessar os servidores DNS fornecidos ou os controladores de domínio do seu domínio. Para corrigir esse problema, atualize a configuração do Active Directory da sua máquina virtual de armazenamento com servidores DNS válidos e uma configuração de rede que permita que o tráfego flua da máquina virtual de armazenamento para o controlador de domínio.

Para resolver esse problema, use o seguinte procedimento:

1. Se somente alguns dos controladores de domínio no Active Directory estiverem acessíveis, por exemplo, devido a limitações geográficas ou firewalls, você poderá adicionar controladores de domínio preferenciais. Usando essa opção, a Amazon FSx tenta entrar em contato com os controladores de domínio preferenciais. Adicione controladores de domínio preferenciais usando o comando `vserver cifs domain preferred-dc add` NetApp ONTAP CLI, da seguinte forma:

   a. Para acessar o ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

b. Insira o seguinte comando no qual:

- `-vserver vserver_name` especifica o nome da máquina virtual de armazenamento (SVM).
- `-domain domain_name` especifica o nome de domínio totalmente qualificado (FQDN) do Active Directory ao qual os controladores de domínio especificados pertencem.
- `-preferred-dc IP_address,…` especifica um ou mais endereços IP dos controladores de domínio preferenciais, como uma lista delimitada por vírgulas, por ordem de preferência.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_name -
domain domain_name -preferred-dc IP_address, …+
```

O comando a seguir adiciona os controladores de domínio 172.17.102.25 e 172.17.102.24 à lista de controladores de domínio preferenciais que o servidor SMB na SVM vs1 usa para gerenciar o acesso externo ao domínio cifs.lab.example.com.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
 cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. Verifique se o seu controlador de domínio pode ser resolvido com o DNS. Use o comando `vserver services access-check dns forward-lookup` NetApp ONTAP CLI para retornar o endereço IP de um nome de host com base na pesquisa no servidor DNS especificado ou na configuração DNS do vserver.

a. Para acessar o ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx for NetApp ONTAP ou SVM executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obter mais informações, consulte Gerenciando sistemas de arquivos com o ONTAP CLI.

b. Entre no modo avançado da CLI do ONTAP usando o comando a seguir.

```
FsxId123456789::> set adv
```

c. Insira o seguinte comando no qual:

- `-vserver vserver_name` especifica o nome da máquina virtual de armazenamento (SVM).
- `-hostname host_name` especifica o nome do host a ser pesquisado no servidor DNS.
- `-node node_name` especifica o nome do nó no qual o comando é executado.
- `-lookup-type` especifica o tipo de endereço IP a ser pesquisado no servidor DNS, o padrão é `all`.

```
FsxId123456789::> vserver services access-check dns forward-lookup \
-vserver vserver_name -node node_name \
-domains domain_name -name-servers dns_server_ip_address \
-hostname host_name
```

3. Analise as informações que você precisa ter ao associar uma SVM a um AD.
4. Analise os requisitos de rede ao associar uma SVM a um AD.
5. Use o procedimento descrito em Requisitos de configuração de rede para atualizar a configuração do AD da SVM usando os endereços IP corretos para os servidores DNS do AD.

A Amazon não FSx consegue se comunicar com seu Active Directory devido a um nome de domínio inválido do Active Directory.

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

A Amazon FSx detectou que o FQDN fornecido é inválido. Para corrigir esse problema, atualize a configuração do Active Directory da sua máquina virtual de armazenamento com um FQDN que atenda aos requisitos de configuração.

Para resolver esse problema, use o seguinte procedimento:

1. Analise os requisitos de nome de domínio do Active Directory on-premises descritos em Informações necessárias ao unir uma SVM a um Active Directory. Certifique-se de que o AD que você está tentando associar atenda a esses requisitos.
2. Use o procedimento descrito em Ingressando SVMs no Active Directory usando a API AWS Management Console, AWS CLI e e tente associar novamente a SVM a um AD. Certifique-se de usar o formato correto para o FQDN do domínio do AD.

A conta de serviço não consegue acessar o grupo de administradores especificado na configuração do Active Directory da SVM

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

A Amazon FSx não consegue aplicar sua configuração do Active Directory. Isso ocorre porque o grupo de administradores fornecido não existe ou não está acessível à conta de serviço fornecida. Para corrigir esse problema, certifique-se de que sua configuração de rede permita o tráfego da SVM para os controladores de domínio e servidores DNS do Active Directory. Em seguida, atualize a configuração do Active Directory da SVM, fornecendo os servidores DNS do Active Directory e especificando um grupo de administradores no domínio que possa ser acessado pela conta de serviço fornecida.

Para resolver esse problema, faça o seguinte:

1. Analise as informações sobre como fornecer um grupo de domínio para realizar ações administrativas na SVM. Verifique se está usando o nome correto do grupo de administradores de domínio do AD.
2. Use o procedimento descrito em Ingressando SVMs no Active Directory usando a API AWS Management Console, AWS CLI e e tente associar novamente a SVM a um AD.

A Amazon não FSx pode se conectar aos controladores de domínio do Active Directory porque a unidade organizacional especificada não existe ou não está acessível

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

FSx A Amazon não consegue estabelecer uma conexão com seu Active Directory. Isso ocorre porque a unidade organizacional especificada não existe ou não está acessível à conta de serviço fornecida. Para corrigir esse problema, atualize a configuração do Active Directory da sua máquina virtual de armazenamento, especificando uma unidade organizacional à qual a conta de serviço tem permissões para se associar.

Para resolver esse problema, faça o seguinte:

1. Analise os pré-requisitos para associar uma SVM a um AD.
2. Analise as informações que você precisa ter ao associar uma SVM a um AD.
3. Tente associar novamente a SVM ao AD usando este procedimento com a unidade organizacional correta.

Não é possível excluir um volume ou uma máquina virtual de armazenamento

Cada sistema FSx de arquivos do ONTAP pode conter uma ou mais máquinas virtuais de armazenamento (SVMs), e cada SVM pode conter um ou mais volumes. Ao excluir um recurso, você deve primeiro garantir que todos os recursos secundários tenham sido excluídos. Por exemplo, antes de excluir uma SVM, você deve primeiro excluir todos os volumes não raiz na SVM.

> **Important**
>
> Você só pode excluir máquinas virtuais de armazenamento usando o FSx console, a API e a CLI da Amazon. Você só pode excluir volumes usando o FSx console, a API ou a CLI da Amazon se o volume tiver os FSx backups da Amazon habilitados.

Para ajudar a proteger seus dados e sua configuração, a Amazon FSx impede a exclusão SVMs e os volumes em determinadas circunstâncias. Se você tentar excluir uma SVM ou volume e sua solicitação de exclusão não for bem-sucedida, a Amazon FSx fornecerá informações no AWS console, AWS Command Line Interface (AWS CLI) e na API sobre o motivo pelo qual o recurso não foi excluído. Depois de resolver a causa da falha de exclusão, você poderá repetir a solicitação de exclusão.

Tópicos

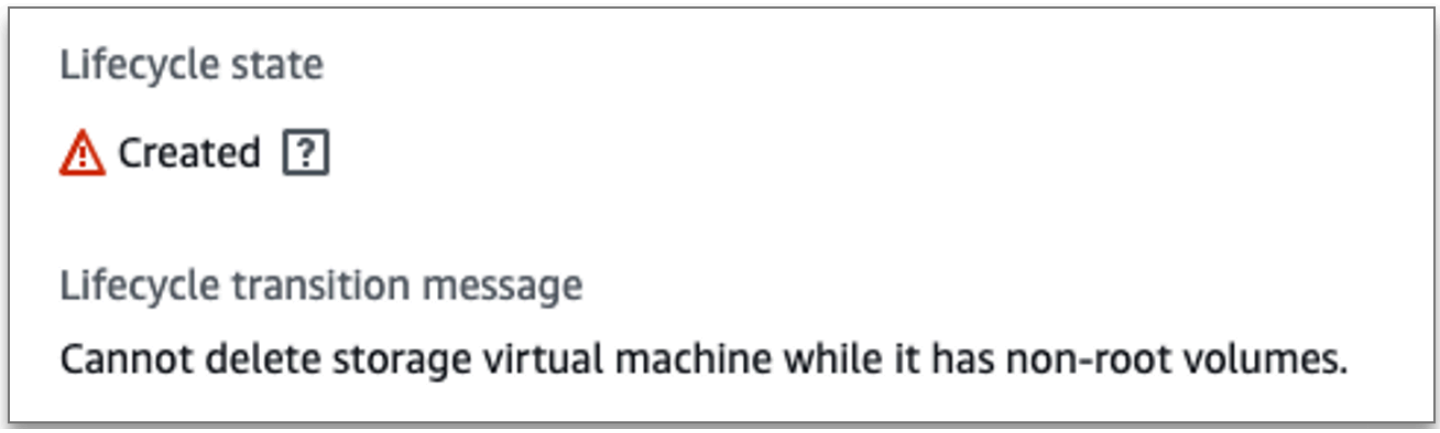
- Identificar falhas em exclusões

- Exclusão de SVM: tabelas de rotas inacessíveis
- Exclusão da SVM: relacionamento entre pares
- SVM ou exclusão de volume: SnapMirror
- Exclusão de SVM: LIF habilitada pelo Kerberos
- Exclusão de SVM: outro motivo
- Exclusão de volume: relacionamento FlexCache

Identificar falhas em exclusões

Quando você exclui um Amazon FSx SVM ou volume, você normalmente vê a transição de `Lifecycle` estado do recurso `DELETING` por até alguns minutos antes que o recurso desapareça do FSx console, da CLI e da API da Amazon.

Se você tentar excluir um recurso e o estado de `Lifecycle` mudar para `DELETING` e depois voltar para `CREATED`, esse comportamento indica que o recurso não foi excluído com êxito. Nesse caso, a Amazon FSx relata um ícone de alerta no console ao lado do estado do `CREATED` ciclo de vida. Escolher o ícone de alerta exibe o motivo da exclusão malsucedida, conforme mostrado no exemplo a seguir.



Os motivos mais comuns pelos quais a Amazon FSx impede a exclusão de SVM e volume são fornecidos nas seções a seguir, com step-by-step instruções sobre como resolver esses problemas.

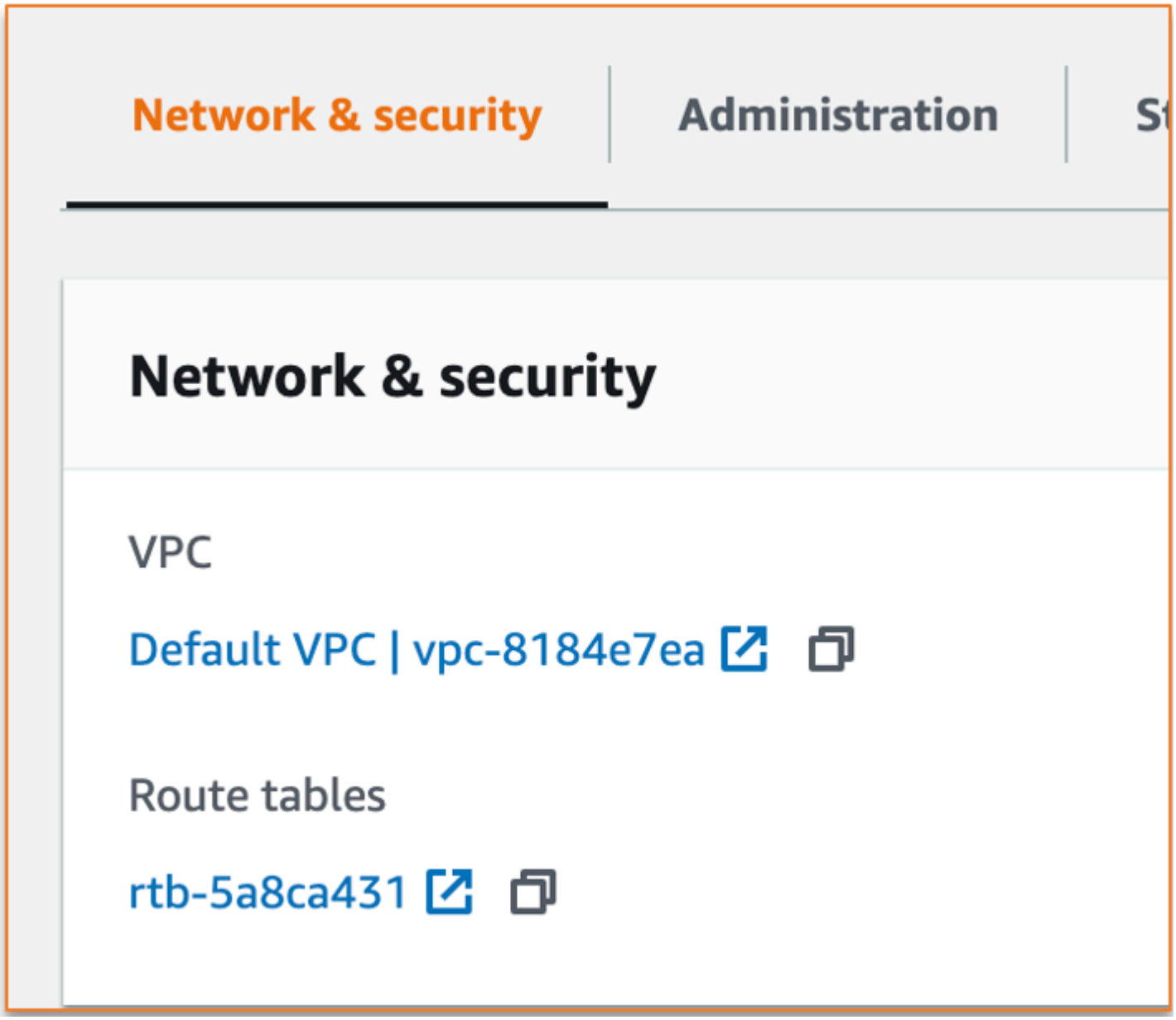
Exclusão de SVM: tabelas de rotas inacessíveis

Cada sistema FSx de arquivos do ONTAP cria uma ou mais entradas na tabela de rotas para fornecer failover e failback automáticos nas zonas de disponibilidade. Por padrão, essas entradas da tabela de rotas são criadas na tabela de rotas padrão da VPC. Opcionalmente, você pode especificar

uma ou mais tabelas de rotas não padrão nas quais FSx as interfaces do ONTAP podem ser criadas. A Amazon FSx marca cada tabela de rotas associada a um sistema de arquivos com uma `AmazonFSx` tag e, se essa tag for removida, poderá FSx impedir que a Amazon exclua recursos. Se essa situação ocorrer, você verá o seguinte `LifecycleTransitionReason`:

```
Amazon FSx is unable to complete the requested storage virtual machine
operation because of an inability to access one or more of the route tables
associated with your file system. Please contact Suporte.
```

Você pode encontrar as tabelas de rotas do seu sistema de arquivos no FSx console da Amazon navegando até a página de resumo do sistema de arquivos, na guia Rede e segurança:



Escolher o link das tabelas de rotas leva você às suas tabelas de rotas. Em seguida, verifique se cada uma das tabelas de rotas associadas ao seu sistema de arquivos está marcada com esse par de chave-valor:

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

Se essa tag não estiver presente, recrie-a e tente excluir a SVM novamente.

Exclusão da SVM: relacionamento entre pares

Se estiver tentando excluir uma SVM ou um volume que faça parte de um relacionamento entre pares, primeiro exclua o relacionamento entre pares antes de excluir a SVM ou o volume. Esse requisito evita que o peering se torne SVMs insalubre. Se a SVM não puder ser excluída por causa de um relacionamento entre pares, você verá o seguinte `LifecycleTransitionReason`:

FSx A Amazon não consegue excluir a máquina virtual de armazenamento porque ela faz parte de uma relação entre pares de SVM ou pares de transição. Exclua o relacionamento e tente novamente.

Você pode excluir relacionamentos entre pares de SVM por meio da CLI do ONTAP. Para acessar a CLI do ONTAP, siga as etapas em Gerenciando sistemas de arquivos com o ONTAP CLI. Usando a CLI do ONTAP, siga as etapas a seguir.

1. Verifique os relacionamentos entre pares de SVM usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

   Se esse comando for executado com êxito, você verá uma saída semelhante à:

```
            Peer        Peer                           Peering        Remote
Vserver     Vserver     State        Peer Cluster      Applications   Vserver
----------- ----------- ------------ ----------------- -------------- ---------
svm_name    test2       peered       FsxId02d81fef0d84734b6
                                                       snapmirror     fsxDest
svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                       snapmirror     fsxDest
2 entries were displayed.
```

2. Exclua cada relacionamento entre pares de SVM usando o comando a seguir. Substitua *svm_name* e *remote_svm_name* pelos seus valores reais.

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

Se esse comando for executado com êxito, você verá a seguinte saída:

```
Info: 'vserver peer delete' command is successful.
```

SVM ou exclusão de volume: SnapMirror

Assim como você não pode excluir uma SVM com um relacionamento entre pares sem primeiro excluir o relacionamento entre pares (consulteExclusão da SVM: relacionamento entre pares), você não pode excluir um SVM que tenha um SnapMirror relacionamento sem primeiro excluir o relacionamento. SnapMirror Para excluir o SnapMirror relacionamento, use a CLI do ONTAP para seguir as etapas a seguir no sistema de arquivos que é o destino do SnapMirror relacionamento. Para acessar a CLI do ONTAP, siga as etapas em Gerenciando sistemas de arquivos com o ONTAP CLI.

> **Note**
>
> FSx Os backups da Amazon são usados SnapMirror para criar point-in-time backups incrementais dos volumes do seu sistema de arquivos. Você não pode excluir essa SnapMirror relação para seus backups na CLI do ONTAP. No entanto, esse relacionamento é excluído automaticamente ao excluir um volume por meio da CLI, da API ou do console da AWS .

1. Liste seus SnapMirror relacionamentos no sistema de arquivos de destino usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

Se esse comando for executado com êxito, você verá uma saída semelhante à:

```
Source            Destination    Mirror  Relationship   Total             Last
Path        Type  Path           State   Status         Progress  Healthy Updated
----------- ---- ------------    ------- -------------- --------- ------- --------
sourceSvm:sourceVol
            XDP  destSvm:destVol Snapmirrored
                                       Idle           -         true    -
```

2. Exclua seu SnapMirror relacionamento executando o comando a seguir no sistema de arquivos de destino.

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

Exclusão de SVM: LIF habilitada pelo Kerberos

Se estiver tentando excluir uma SVM que tenha uma interface lógica (LIF) com o Kerberos habilitado, primeiro desative o Kerberos nessa LIF antes de excluir a SVM.

Você pode desabilitar o Kerberos em uma LIF por meio da CLI do ONTAP. Para acessar a CLI do ONTAP, siga as etapas em Gerenciando sistemas de arquivos com o ONTAP CLI.

1. Entre no modo de diagnóstico na CLI do ONTAP usando o comando a seguir.

```
FsxId123456789abcdef::> set diag
```

Quando for solicitado que continue, insira **y**.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

2. Verifique quais interfaces têm o Kerberos habilitado. Substitua *svm_name* pelo nome da sua SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Se esse comando for executado com êxito, você verá uma saída semelhante à:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    enabled
5 entries were displayed.
```

3. Desabilite a LIF do Kerberos usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM. Você precisará fornecer o nome de usuário e a senha do Active Directory usados para associar essa SVM ao Active Directory.

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

Se esse comando for executado com êxito, você verá a saída a seguir. Forneça o nome de usuário e a senha do Active Directory usados para associar essa SVM ao Active Directory. Quando for solicitado que continue, insira **y**.

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *************

Warning: This command deletes the service principal name from the machine account
 on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. Verifique se o Kerberos está desabilitado na SVM usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Se esse comando for executado com êxito, você verá uma saída semelhante à:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    disabled
5 entries were displayed.
```

5. Se a interface for mostrada como`disabled`, tente excluir a SVM novamente por meio da AWS CLI, da API ou do console.

   Se você não conseguiu excluir a LIF usando os comandos anteriores, poderá forçar a exclusão da LIF do Kerberos usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

   > **Important**
   >
   > O comando a seguir pode prender o objeto computacional da SVM no Active Directory.

   ```
   FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
    nfs_smb_management_1 -force true
   ```

   Se esse comando for executado com êxito, você verá uma saída semelhante à mostrada a seguir. Quando for solicitado que continue, insira **y**.

   ```
   (vserver nfs kerberos interface disable)

   Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver
    "svm_name" will be deleted.
   The corresponding account on the KDC will not be deleted. Do you want to continue?
    {y|n}: y
   ```

Exclusão de SVM: outro motivo

FSx para ONTAP, SVMs crie um objeto de computador no Active Directory quando eles se juntarem ao Active Directory. Em alguns casos, talvez você queira desassociar manualmente uma SVM do Active Directory usando a CLI do ONTAP. Para acessar a CLI do ONTAP, siga as etapas em Gerenciando sistemas de arquivos com o ONTAP CLI, fazendo login na CLI do ONTAP no nível do

sistema de arquivos com as credenciais de `fsxadmin`. Usando a CLI do ONTAP, siga as etapas a seguir para desassociar uma SVM do Active Directory.

> **Important**
>
> Esse procedimento pode prender o objeto computacional da SVM no Active Directory.

1. Entre no modo avançado na CLI do ONTAP usando o comando a seguir.

   ```
   FsxId123456789abcdef::> set adv
   ```

   Após executar esse comando, você verá essa saída. Insira **y** para continuar.

   ```
   Warning: These advanced commands are potentially dangerous; use them only when
         directed to do so by NetApp personnel.
         Do you want to continue? {y|n}: y
   ```

2. Exclua o DNS do Active Directory usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

   ```
   FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
    delete -vserver svm_name -lif nfs_smb_management_1
   ```

   > **Note**
   >
   > Se o registro DNS já tiver sido excluído ou se o servidor DNS estiver inacessível, esse comando falhará. Se isso acontecer, prossiga para a próxima etapa.

3. Desabilite o DNS usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

   ```
   FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
   vserver svm_name -is-enabled false -use-secure false
   ```

   Se esse comando for executado com êxito, você verá a seguinte saída:

   ```
   Warning: DNS updates for Vserver "svm_name" are now disabled.
        Any LIFs that are subsequently modified or deleted
        can result in a stale DNS entry on the DNS server,
   ```

```
    even when DNS updates are enabled again.
```

4. Desassocie o dispositivo do Active Directory. Substitua *svm_name* pelo nome da sua SVM.

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

Após executar esse comando, você verá a saída a seguir, na qual *CORP.EXAMPLE.COM* é substituído pelo nome do seu domínio. Quando for solicitado, insira o nome de usuário e senha. Quando perguntado se deseja excluir o servidor, digite **y**.

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
    Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
 server.
    Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

Exclusão de volume: relacionamento FlexCache

Você não pode excluir volumes que são os volumes de origem de um FlexCache relacionamento, a menos que primeiro exclua o relacionamento de cache. Para determinar quais volumes têm uma FlexCache relação, você pode usar a CLI do ONTAP. Para acessar a CLI do ONTAP, siga as etapas em Gerenciando sistemas de arquivos com o ONTAP CLI.

1. Verifique os FlexCache relacionamentos usando o comando a seguir.

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. Exclua qualquer relacionamento de cache usando o comando a seguir. Substitua *dest_svm_name* e *dest_vol_name* pelos seus valores reais.

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. Após excluir o relacionamento do cache, tente excluir a SVM por meio da CLI, da API ou do console da AWS novamente.

Seu volume está em um **`MISCONFIGURED`** estado

Há várias causas possíveis para um volume ONTAP entrar em um `MISCONFIGURED` estado, descritas nos tópicos a seguir.

Seu volume está mais de 98% cheio

Seu sistema de arquivos atualmente contém um volume que está mais de 98% cheio. Recomendamos que você não exceda 95% de utilização do seu volume de forma contínua. Se você não liberar espaço no volume antes da próxima janela de manutenção do seu sistema de arquivos, a Amazon FSx desativará o bloqueio oportunista do volume, quebrando quaisquer “oplocks” existentes. A Amazon FSx reativará os oplocks no volume após a conclusão do processo de correção. Para evitar isso, reduza a utilização da capacidade de armazenamento do volume para menos de 98%. Algumas das maneiras de conseguir isso incluem:

- Aumentando o tamanho do volume.
- Excluindo dados desnecessários.
- Excluindo instantâneos desnecessários.

Para ter mais informações, consulte Como atualizar a capacidade de armazenamento e Exclusão de snapshots.

Seu volume off-line tem um iSCSI LUN ou um namespace /TCP NVMe

Seu sistema de arquivos atualmente hospeda um volume que está em um estado off-line, e esse volume contém um LUN iSCSI, ou um namespace NVMe /TCP, ou ambos. Recomendamos que você mantenha os volumes on-line continuamente. Se você não colocar esse volume on-line antes da próxima janela de manutenção do seu sistema de arquivos, a Amazon o FSx colocará temporariamente on-line durante a operação de correção. Para evitar isso, conecte ou exclua o volume.

Para colocar um volume off-line novamente on-line, use o `volume online` ONTAP Comando CLI, conforme mostrado no exemplo a seguir. Se existir apenas um SVM (Vserver), você não precisará especificar o `-vserver` parâmetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Seu volume off-line é um FlexCache origem

Seu sistema de arquivos contém um volume de FlexCache origem que está em um estado off-line. Recomendamos que você mantenha os volumes on-line continuamente. Se você não colocar esse volume on-line antes da próxima janela de manutenção do seu sistema de arquivos, a Amazon o FSx colocará temporariamente on-line durante a operação de correção. Durante esse período, é possível que os dados sejam gravados de volta no volume de FlexCache origem com os dados do volume de cache. Para evitar isso, conecte ou exclua o volume.

Para colocar um volume off-line novamente on-line, use o `volume online` ONTAP Comando CLI, conforme mostrado no exemplo a seguir. Se existir apenas um SVM (Vserver), você não precisará especificar o `-vserver` parâmetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Seu volume off-line faz parte de um SnapMirror relação

Seu sistema de arquivos atualmente hospeda um volume que está em um estado off-line, e esse volume é um SnapMirror origem ou destino. Recomendamos que você mantenha os volumes on-line continuamente. Se você não colocar esse volume on-line antes da próxima janela de manutenção do seu sistema de arquivos, a Amazon o FSx colocará temporariamente on-line durante a operação de correção e interromperá o SnapMirror relacionamento. Durante esse período, é possível que os dados sejam gravados no SnapMirror volume de destino com dados do SnapMirror volume de origem. Para evitar isso, conecte ou exclua o volume.

Para colocar um volume off-line novamente on-line, use o `volume online` ONTAP Comando CLI, conforme mostrado no exemplo a seguir. Se existir apenas um SVM (Vserver), você não precisará especificar o `-vserver` parâmetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Seu volume restrito contém um iSCSI LUN ou um namespace /TCP NVMe

Atualmente, seu sistema de arquivos hospeda um volume que está em um estado restrito e esse volume contém um LUN iSCSI, um namespace NVMe /TCP ou ambos. Recomendamos que você mantenha os volumes on-line continuamente. Se você não colocar esse volume on-line antes da próxima janela de manutenção do seu sistema de arquivos, a Amazon o FSx colocará temporariamente on-line durante a operação de correção. Para evitar isso, conecte ou exclua o volume.

Para colocar um volume off-line novamente on-line, use o `volume online` ONTAP Comando CLI, conforme mostrado no exemplo a seguir. Se existir apenas um SVM (Vserver), você não precisará especificar o `-vserver` parâmetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Seu volume restrito é uma FlexCache origem

Seu sistema de arquivos contém um volume de FlexCache origem que está em um estado restrito. Recomendamos que você mantenha os volumes on-line continuamente. Se você não colocar esse volume on-line antes da próxima janela de manutenção do seu sistema de arquivos, a Amazon o FSx colocará temporariamente on-line durante a operação de correção. Durante esse período, é possível que os dados sejam gravados de volta no volume de FlexCache origem com os dados do volume de cache. Para evitar isso, conecte ou exclua o volume.

Para colocar um volume off-line novamente on-line, use o `volume online` ONTAP Comando CLI, conforme mostrado no exemplo a seguir. Se existir apenas um SVM (Vserver), você não precisará especificar o `-vserver` parâmetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Seu volume restrito faz parte de um SnapMirror relação

Seu sistema de arquivos atualmente hospeda um volume que está em um estado restrito, e esse volume é um SnapMirror origem ou destino. Recomendamos que você mantenha os volumes on-line

continuamente. Se você não colocar esse volume on-line antes da próxima janela de manutenção do seu sistema de arquivos, a Amazon o FSx colocará temporariamente on-line durante a operação de correção e interromperá o SnapMirror relacionamento. Durante esse período, é possível que os dados sejam gravados no SnapMirror volume de destino com dados do SnapMirror volume de origem. Para evitar isso, conecte ou exclua o volume.

Para colocar um volume off-line novamente on-line, use o `volume online` ONTAP Comando CLI, conforme mostrado no exemplo a seguir. Se existir apenas um SVM (Vserver), você não precisará especificar o `-vserver` parâmetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Seu volume tem capacidade de armazenamento insuficiente

Se estiver ficando sem espaço nos seus volumes, poderá usar os procedimentos mostrados aqui para diagnosticar e resolver a situação.

Tópicos

- Determine como a capacidade de armazenamento do volume está sendo usada
- Como aumentar a capacidade de armazenamento de um volume
- Como usar o dimensionamento automático de volume
- O armazenamento principal do sistema de arquivos está cheio
- Exclusão de snapshots
- Como aumentar a capacidade máxima de arquivos de um volume

Determine como a capacidade de armazenamento do volume está sendo usada

Você pode ver como a capacidade de armazenamento do seu volume está sendo consumida usando o comando `volume show-space` NetApp ONTAP CLI. Essas informações podem ajudar a tomar decisões sobre como recuperar ou conservar a capacidade de armazenamento do volume. Para obter mais informações, consulte Monitorar a capacidade de armazenamento de um volume (console).

Como aumentar a capacidade de armazenamento de um volume

Você pode aumentar a capacidade de armazenamento de um volume usando o FSx console da Amazon e a FSx API da Amazon. AWS CLI Para obter mais informações sobre como atualizar um volume com maior capacidade, consulte Atualizar volumes.

Como alternativa, você pode aumentar a capacidade de armazenamento de um volume usando o comando `volume modify` NetApp ONTAP CLI. Para obter mais informações, consulte Alterar a capacidade de armazenamento de um volume (console).

Como usar o dimensionamento automático de volume

Você pode usar o dimensionamento automático de volume para que um volume cresça automaticamente em uma quantidade especificada ou até um tamanho especificado quando atingir um limite de espaço usado. Você pode fazer isso para tipos de FlexVol volume, que é o tipo de volume padrão FSx para ONTAP, usando o comando `volume autosize` NetApp ONTAP CLI. Para obter mais informações, consulte Habilitar o dimensionamento automático.

O armazenamento principal do sistema de arquivos está cheio

Se o FSx armazenamento principal do sistema de arquivos do ONTAP estiver cheio, você não poderá adicionar mais dados aos volumes do sistema de arquivos, mesmo que um volume mostre que tem capacidade de armazenamento disponível suficiente. Você pode ver a quantidade de capacidade de armazenamento primário disponível na guia Monitoramento e desempenho na página de detalhes do sistema de arquivos no FSx console da Amazon. Para obter mais informações, consulte Monitorar a utilização do armazenamento SSD.

Para resolver esse problema, você pode aumentar o tamanho do nível de armazenamento principal do sistema de arquivos. Para obter mais informações, consulte Atualização do armazenamento SSD e IOPS do sistema de arquivos.

Exclusão de snapshots

Os snapshots são habilitados por padrão nos volumes, usando a política de snapshots padrão. Os snapshots são armazenados no diretório `.snapshot` na raiz de um volume. Você pode gerenciar a capacidade de armazenamento de volumes em relação aos snapshots das seguintes maneiras:

- Excluir os snapshots manualmente: recupere a capacidade de armazenamento excluindo os snapshots manualmente.

- Criar uma política de exclusão automática de snapshots: crie uma política que exclua os snapshots de forma mais agressiva do que a política de snapshots padrão.
- Desativar os snapshots automáticos: conserve a capacidade de armazenamento desativando os snapshots automáticos.

Ao excluir um snapshot, você não recupera a quantidade de armazenamento igual ao tamanho do snapshot que você está excluindo. Você pode ver a quantidade de armazenamento que você pode recuperar ao excluir um snapshot usando o volume snapshot compute-reclaimable -vserver ONTAP Comando CLI, usando seus dados para substituir *svm_namevol_name*, e. *snapshot_name*

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

Para obter mais informações sobre como excluir snapshots e gerenciar políticas de snapshots para conservar a capacidade de armazenamento, consulte Exclusão de snapshots.

Como aumentar a capacidade máxima de arquivos de um volume

Um volume FSx para ONTAP pode ficar sem capacidade de arquivo quando o número de inodes ou ponteiros de arquivo disponíveis estiver esgotado. Por padrão, o número de inodes disponíveis em um volume é de 1 para cada 32 KiB de tamanho do volume. Para obter mais informações, consulte Capacidade do arquivo de volumes.

O número de inodes em um volume aumenta proporcionalmente à capacidade de armazenamento do volume, até um limite de 648 GiB. Por padrão, todos os volumes com capacidade de armazenamento de 648 GiB ou mais têm o mesmo número de inodes, 21.251.126. Para visualizar a capacidade máxima de arquivos de um volume, consulte Monitorar a capacidade de arquivos de um volume.

Se você criar um volume maior que 648 GiB e quiser ter mais de 21.251.126 inodes, deverá aumentar o número máximo de arquivos no volume manualmente. Se a capacidade de armazenamento do volume estiver acabando, você poderá verificar a capacidade máxima de arquivos. Se estiver se aproximando da capacidade de arquivos, você poderá aumentá-la manualmente. Para obter mais informações, consulte Aumentar o número máximo de arquivos em um volume (CLI do ONTAP).

Seus backups falham devido à capacidade insuficiente de volume

Os backups diários automáticos do seu volume falham com a seguinte mensagem de erro:

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

Os backups diários automáticos estão falhando porque não há capacidade suficiente de armazenamento livre no volume. Para mitigar essa condição, você precisará liberar capacidade de armazenamento no volume. Dependendo da sua situação, você pode fazer isso usando uma ou mais das seguintes opções:

- Aumentar a capacidade de armazenamento do volume
- Aumentar a reserva de snapshots do volume
- Desativar a exclusão automática de snapshots
- Não exclua o snapshot de backup usando a CLI do ONTAP

Corrigir problemas de rede

Se estiver enfrentando problemas de rede, poderá usar os procedimentos mostrados aqui para diagnosticar o problema.

Você deseja capturar um rastreamento de pacote

O rastreamento de pacotes é o processo de verificar o caminho de um pacote pelas camadas até seu destino. Você controla o processo de rastreamento de pacotes com o seguinte NetApp ONTAP Comandos da CLI:

- network tcpdump start: inicia o rastreamento de pacotes
- network tcpdump show: mostra os rastreamentos de pacotes atualmente em execução
- network tcpdump stop: interrompe um rastreamento de pacotes em execução

Esses comandos estão disponíveis para usuários que tenham o perfil `fsxadmin` no sistema de arquivos.

Capturar um rastreamento de pacotes do sistema de arquivos

1. Para usar SSH no NetApp ONTAP CLI do seu sistema de arquivos, siga as etapas documentadas na Usar o NetApp ONTAP CLI seção do Guia do usuário do Amazon FSx for NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Insira o nível de privilégio do diagnóstico na CLI do ONTAP usando o comando a seguir.

```
::> set diag
```

Quando for solicitado que continue, insira `y`.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

3. Identifique o local no sistema de arquivos onde deseja salvar o rastreamento de pacotes. O volume deve estar on-line e montado no namespace com um caminho de junção válido. Use o seguinte comando para verificar se há volumes que atendem a esses critérios:

```
::*> volume show -junction-path !- -fields junction-path
vserver volume    junction-path
------- --------- -------------
fsx     test_vol1 /test_vol1
fsx     test_vol2 /test_vol2
fsx     test_vol2 /test_vol3
```

4. Inicie o rastreamento com os argumentos mínimos necessários. Substitua o seguinte:

- *node_name*Substitua pelo nome do nó (por exemplo,`FsxId01234567890abcdef-01`).
- *svm_name*Substitua pelo nome da sua máquina virtual de armazenamento (por exemplo,`fsx`).
- *junction_path_name*Substitua pelo nome do volume (por exemplo,`test-vol1`).

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
 e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
 packet traces are occurring. Use the
```

```
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
 disable Snapshots on the
tcpdump destination volume.
```

> **Important**
>
> Os rastreamentos de pacotes só podem ser capturados na interface `e0e` e no espaço `Default` de IP. No FSx ONTAP, todo o tráfego de rede usa a `e0e` interface.

Ao usar o rastreamento de pacotes, lembre-se dos seguintes pontos:

- Ao iniciar um rastreamento de pacotes, você deve incluir o caminho para onde deseja armazenar os arquivos de rastreamento, neste formato: /clus//*svm_namejunction-path-name*
- Opcionalmente, forneça o nome do arquivo para o rastreamento do pacote. Se o nome_filtro não for especificado, ele será gerado automaticamente no formato: *node-name* _ _ *port-name* .trc *yyyymmdd_hhmmss*
- Se rastreamentos cumulativos forem especificados, o filter_name será sufixado com um número que indica a posição na sequência de rotação.
- A CLI do ONTAP também aceita os seguintes argumentos -pass-through opcionais:

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
<filter-expression>
```

- Para obter informações sobre expressões de filtro, consulte a página inicial de pcap-filter(7).

5. Veja os rastreamentos em andamento:

```
::*> debug network tcpdump show
Node                    IPspace  Port     Filename
```

```
----------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. Pare o rastreamento:

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

7. Retorne ao nível de privilégio de administrador:

```
::*> set -priv admin
::>
```

8. Acesse os rastreamentos de pacotes.

   Seus rastreamentos de pacotes são armazenados no volume especificado usando o comando debug network tcpdump start e podem ser acessados por meio da exportação de NFS ou de um compartilhamento SMB que corresponda a esse volume.

Para obter mais informações sobre a captura de rastreamentos de pacotes, consulte Como usar o debug network dump no ONTAP 9.10+ no NetApp Knowledge Base.

Histórico de documentos da Amazon FSx para NetApp ONTAP

- Versão da API: 1/3/2018
- Última atualização da documentação: 9 de junho de 2025

A tabela a seguir descreve mudanças importantes no Guia do usuário do Amazon FSx NetApp ONTAP. Para receber notificações sobre atualizações da documentação, inscreva-se no feed RSS.

Alteração	Descrição	Data
FSx for ONTAP oferece suporte ao Amazon Elastic Service VMware	FSx for ONTAP agora pode ser usado como um armazenamento de dados externo para o Amazon EVS. Para obter mais informações, consulte Usando o Amazon Elastic VMware Service com FSx o ONTAP.	9 de junho de 2025
Região da AWS Suporte adicional adicionado	A segunda geração (Multi-AZ 2 e Single-AZ 2) FSx para sistemas de arquivos ONTAP agora está disponível na Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Mumbai). Para obter mais informações, consulte Disponibilidade por Região da AWS.	2 de junho de 2025
Support adicionado para o modo FlexCache write-back	FSx para volumes ONTAP agora suportam o modo FlexCache write-back. Para obter mais informações,	28 de maio de 2025

	consulte Replicando seus dados com FlexCache.	
A Amazon FSx atualizou a política FSx FullAccess AWS gerenciada da Amazon	A política FSx FullAccess gerenciada da Amazon foi atualizada para adicionar as `fsx:DetachAndDeleteS3AccessPoint` permissões `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , `fsx:UpdateS3AccessPointAttachments` , e.	28 de maio de 2025
A Amazon FSx atualizou a política FSx ConsoleFullAccess AWS gerenciada da Amazon	A política FSx ConsoleFullAccess gerenciada da Amazon foi atualizada para adicionar as `fsx:DetachAndDeleteS3AccessPoint` permissões `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , `fsx:UpdateS3AccessPointAttachments` , e.	28 de maio de 2025

Região da AWS Suporte adicional adicionado	FSx Os sistemas de arquivos para ONTAP agora estão disponíveis na Ásia-Pacífico (Tailândia) e no México (Central). Para obter mais informações, consulte Disponibilidade por Região da AWS.	8 de maio de 2025
A Proteção Autônoma contra Ransomware (ARP) agora é suportada	O ARP, um recurso NetApp baseado em IA que monitora e protege contra ataques de ransomware e malware, agora é suportado pelo FSx for ONTAP. Para obter mais informações, consulte Protegendo seus dados com o Autonomous Ransomware Protection	7 de abril de 2025
O novo tópico no Guia do Usuário do FSx for ONTAP descreve como configurar um servidor SMB em um grupo de trabalho	A configuração de servidores SMB em um grupo de trabalho descreve como configurar um servidor SMB no grupo de trabalho em uma SVM como alternativa à associação de uma SVM a um Microsoft Active Directory.	4 de março de 2025

A Amazon FSx atualizou a política FSx ConsoleReadOnlyAccess AWS gerenciada da Amazon	A Amazon FSx atualizou a FSx ConsoleReadOnlyAccess política da Amazon para adicionar a `ec2:DescribeNetworkInterfaces` permissão. Para obter mais informações, consulte a FSx ConsoleReadOnlyAccess política da Amazon.	25 de fevereiro de 2025
Agora há suporte para Harvest painéis adicionais	Agora, Harvest painéis adicionais são compatíveis com o ONTAP, incluindo painéis que não estão habilitados por FSx padrão. Uma lista de painéis que o FSx ONTAP não suporta também foi adicionada. Para obter mais informações, consulte Monitoramento de sistemas FSx de arquivos ONTAP usando Harvest e Grafana.	18 de fevereiro de 2025
Novo tópico sobre relatórios FSx de faturamento e uso do ONTAP adicionado ao FSx Guia do usuário do ONTAP	O tópico Relatórios de AWS faturamento e uso do ONTAP explica como acessar o faturamento dos relatórios de uso dos sistemas de FSx arquivos ONTAP no console. FSx Gerenciamento de Faturamento e Custos da AWS Ele também fornece todos os tipos de uso em ambos os relatórios que são específicos do ONTAP. FSx	13 de fevereiro de 2025

Support adicionado para endpoints de interface VPC de pilha dupla para Amazon FSx	Agora você pode criar endpoints de interface VPC de pilha dupla para a FSx Amazon com endereços IP IPv4 IPv6 e nomes DNS. Para obter mais informações, consulte os FSx endpoints ONTAP e VPC de interface.	7 de fevereiro de 2025
Support adicionado para endpoints de API de pilha dupla	A API FSx de serviços da Amazon para criar e gerenciar sistemas de arquivos tem novos endpoints de pilha dupla. Para obter mais informações, consulte os endpoints da API na Amazon FSx API Reference.	7 de fevereiro de 2025
A Amazon FSx atualizou a política FSx ConsoleFullAccess AWS gerenciada da Amazon	A Amazon FSx atualizou a FSx ConsoleFullAccess política da Amazon para adicionar a `ec2:DescribeNetworkInterfaces` permissão. Para obter mais informações, consulte a FSx ConsoleFullAccess política da Amazon.	7 de fevereiro de 2025

Novo tópico publicado , Replicando dados com FlexCache	Foi publicado um novo tópico descrevendo como replicar os dados em um sistema de arquivos ONTAP local para um sistema de arquivos ONTAP FSx para uso do ONTAP. FlexCache Para obter mais informações, consulte Replicando dados com FlexCache.	19 de dezembro de 2024
Adição de compatibilidade com sistemas de arquivos de segunda geração	Agora, você pode criar sistemas de arquivos Single-AZ e Multi-AZ de segunda geração. Um único par de alta disponibilidade (HA) agora oferece até 6% GBps da capacidade de taxa de transferência e 200.000 IOPS de SSD. Para obter mais informações, consulte High-availability (HA) pairs.	9 de julho de 2024
Adição de compatibilidade com leitura de dados de um volume enquanto eles estão sendo restaurados de um backup	Agora, você pode montar um volume com acesso somente leitura aos dados de arquivo enquanto ele estiver sendo restaurado de um backup em sistemas de arquivos de segunda geração. Para obter mais informações, consulte Restaurando backups em um novo volume.	9 de julho de 2024

Adição de compatibilidade com o ajuste da capacidade de throughput em sistemas de arquivos de segunda geração	Agora, você pode ajustar a capacidade de throughput de seus sistemas de arquivos de segunda geração após a criação. Para obter mais informações, consulte Como gerenciar a capacidade de throughput.	9 de julho de 2024
Adição de compatibilidade com a adição de pares de HA a sistemas de arquivos Single-AZ de segunda geração	Agora, você pode adicionar pares de HA aos sistemas de arquivos Single-AZ de segunda geração após a criação. Você pode ter até 12 pares de HA em um sistema de arquivos Single-AZ de segunda geração. Para obter mais informações, consulte Adding high-availability (HA) pairs.	9 de julho de 2024
Support adicionado para o protocolo Non-Volatile Memory Express over TCP (/TCP) NVMe	Agora você pode usar o NVMe/TCP protocolo para transporte de dados na Amazon FSx para sistemas de arquivos NetApp ONTAP. Para obter mais informações, consulte Usando protocolos de armazenamento em bloco	9 de julho de 2024

Adição de compatibilidade com o perfil `fsxadmin-readonly` de usuários administrativos do sistema de arquivos	Agora, o perfil `fsxadmin-readonly` está disponível para usuários administrativos do sistema de arquivos do ONTAP e pode ser usado para aplicações de monitoramento do sistema de arquivos, como NetApp Harvest. Para obter mais informações, consulte Funções e usuários do administrador do sistema de arquivos.	30 de abril de 2024
Adição de compatibilidade com autenticação de chave pública SSH para usuários administrativos de domínio do Windows	Agora, você pode usar a autenticação de chave pública SSH com o sistema de arquivos e usuários SVM de domínio do Active Directory . Para obter mais informações, consulte Configuring Active Directory authentication for ONTAP users.	30 de abril de 2024

Adição de compatibilidade com 12 pares de HA em sistemas de arquivos com escalabilidade horizontal	A Amazon FSx for NetApp ONTAP adicionou suporte para 12 pares de HA em sistemas de arquivos escaláveis. Sistemas de arquivos com 12 pares de HA podem fornecer até 72% GBps da capacidade de taxa de transferência e 2.400.000 IOPS de SSD em 12 pares de alta disponibilidade (HA). Para obter mais informaçõ es, consulte Pares de alta disponibilidade (HA) e o desempenho do Amazon FSx for NetApp ONTAP.	4 de março de 2024
Adição de compatibilidade com o modo de gravação em nuvem	O Amazon FSx for NetApp ONTAP adicionou suporte ao modo de gravação em nuvem para volumes. Para obter mais informações, consulte Enabling cloud write mode on a volume.	6 de fevereiro de 2024
Support adicionado para backup de FlexGroup volumes com AWS Backup	Agora você pode usar AWS Backup para fazer backup e restaurar FlexGroup volumes em seus sistemas de arquivos FSx para ONTAP. Para obter mais informações, consulte Usando AWS Backup com a Amazon FSx.	11 de janeiro de 2024

A Amazon FSx FSx FullAccess atualizou as políticas FSx ServiceRolePolicy AWS gerenciadas da Amazon FSx ConsoleFullAccess FSx ReadOnlyAccess FSxConsoleReadOnlyAccess, Amazon, Amazon e Amazon	A Amazon FSx atualizou as FSx ServiceRolePolicy políticas da Amazon FSx FullAccess FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon, Amazon FSxConsoleReadOnlyAccess, Amazon e Amazon para adicionar a `ec2:GetSecurityGroupsForVpc` permissão. Para obter mais informações, consulte as FSx atualizações da Amazon para políticas AWS gerenciadas.	9 de janeiro de 2024
A Amazon FSx atualizou a Amazon FSx FullAccess e as políticas FSx ConsoleFullAccess AWS gerenciadas pela Amazon	A Amazon FSx atualizou as FSx ConsoleFullAccess políticas da Amazon FSx FullAccess e da Amazon para adicionar a `ManageCrossAccountDataReplication` ação. Para obter mais informações, consulte as FSx atualizações da Amazon para políticas AWS gerenciadas.	20 de dezembro de 2023
Adição de compatibilidade com métricas de expansão	FSx for ONTAP agora fornece CloudWatch métricas da Amazon para sistemas de arquivos com vários pares de HA. Para obter mais informações, consulte Scale-out file system metrics.	26 de novembro de 2023

Adição de compatibilidade com sistemas de arquivos com aumento horizontal da escala	A Amazon FSx for NetApp ONTAP adicionou suporte para sistemas de arquivos escaláveis que podem fornecer até 36% GBps da capacidade de taxa de transferência e 1.200.000 IOPS de SSD em seis pares de alta disponibilidade (HA). Para obter mais informaçõ es, consulte Pares de alta disponibilidade (HA) e o desempenho do Amazon FSx for NetApp ONTAP.	26 de novembro de 2023
Support adicionado para FlexGroup volumes	A Amazon FSx for NetApp ONTAP adicionou suporte para FlexGroup volumes. Para obter mais informações, consulte Volume styles.	26 de novembro de 2023
Adição de compatibilidade com VPC compartilhada para sistemas de arquivos Multi-AZ	Agora, as contas de participa ntes podem criar sistemas de arquivos Multi-AZ em uma VPC que tenha sido compartil hada com elas. As contas do proprietário podem gerenciar esse recurso no FSx console, na CLI e na API da Amazon. Para obter mais informações, consulte Criação de sistemas FSx de arquivos ONTAP em sub-redes compartilhadas	26 de novembro de 2023

A Amazon FSx atualizou a Amazon FSx FullAccess e as políticas FSx ConsoleFullAccess AWS gerenciadas pela Amazon	A Amazon FSx atualizou as FSx ConsoleFullAccess políticas da Amazon FSx FullAccess e da Amazon para adicionar a `fsx:CopySnapshotAndUpdateVolume` permissão. Para obter mais informações, consulte as FSx atualizações da Amazon para políticas AWS gerenciadas.	26 de novembro de 2023
A Amazon FSx atualizou a Amazon FSx FullAccess e as políticas FSx ConsoleFullAccess AWS gerenciadas pela Amazon	A Amazon FSx atualizou as FSx ConsoleFullAccess políticas da Amazon FSx FullAccess e da Amazon para adicionar as `fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` permissões e. Para obter mais informações, consulte as FSx atualizações da Amazon para políticas AWS gerenciadas.	14 de novembro de 2023

Suporte adicionado para criar perfis e usuários adicionais do ONTAP	O Amazon FSx for NetApp ONTAP agora oferece suporte à criação de funções e usuários adicionais do ONTAP para definir os recursos e privilégios do usuário ao usar a CLI e a API REST do ONTAP. Para obter mais informações, consulte Funções e usuários na Amazon FSx para NetApp ONTAP.	6 de setembro de 2023
Support adicionado para CloudWatch métricas adicionais e um painel de monitoramento aprimorado	FSx o for ONTAP agora fornece métricas de desempenho adicionais e um painel de monitoramento aprimorado para melhorar a visibilidade da atividade do sistema de arquivos. Para obter mais informações, consulte Monitoramento com CloudWatch.	17 de agosto de 2023
A Amazon FSx atualizou a política FSx ServiceRolePolicy AWS gerenciada da Amazon	A Amazon FSx atualizou a `cloudwatch:PutMetricData` permissão na Amazon FSxServiceRolePolicy. Para obter mais informações, consulte as FSx atualizações da Amazon para políticas AWS gerenciadas.	24 de julho de 2023

Support adicionado para usar o NetApp System Manager diretamente	Você pode gerenciar seus sistemas FSx de arquivos do ONTAP usando System Manager diretamente deNetApp BlueXP. Para obter mais informações, consulte Usando o NetApp System Manager com o BlueXP.	13 de julho de 2023
Suporte adicionado para monitorar eventos do EMS	Você pode monitorar os eventos do sistema FSx de arquivos ONTAP usando o NetApp ONTAP nativo. Events Management System (EMS) Você pode visualizar eventos do EMS usando a CLI do NetApp ONTAP. Para obter mais informações, consulte Monitoramento FSx de eventos do ONTAP EMS.	13 de julho de 2023
Suporte adicionado para o SnapLock	FSx for ONTAP agora suporta SnapLock volumes. SnapLockpermite que você proteja seus arquivos fazendo a transição para o estado WORM (Write Once, Read Many), o que impede modificações ou exclusões por um período de retenção especificado. FSx for ONTAP suporta os modos de retenção Compliance e Enterprise com SnapLock. Para obter mais informações, consulte Trabalhando com SnapLock.	13 de julho de 2023

Support adicionado para IPsec criptografia de dados em trânsito	FSx o for ONTAP agora suporta o uso de IPsec criptografia para criptografar dados em trânsito entre sistemas de arquivos e clientes conectados. Para obter mais informações, consulte Configurando IPsec usando a autenticação PSK e Configurando IPsec usando a autenticação de certificado.	13 de julho de 2023
O tamanho máximo do volume aumentou	FSx para ONTAP atualizou o tamanho máximo de um volume de 100 TB para 300 TB. Para obter mais informações, consulte Ativar o dimensionamento automático de volumes.	13 de julho de 2023
A Amazon FSx atualizou a política FSx FullAccess AWS gerenciada da Amazon	A Amazon FSx atualizou a FSx FullAccess política da Amazon para remover a `fsx:*` permissão e adicionar `fsx` ações específicas. Para obter mais informações, consulte a FSx FullAccess política da Amazon.	13 de julho de 2023
A Amazon FSx atualizou a política FSx ConsoleFullAccess AWS gerenciada da Amazon	A Amazon FSx atualizou a FSx ConsoleFullAccess política da Amazon para remover a `fsx:*` permissão e adicionar `fsx` ações específicas. Para obter mais informações, consulte a FSx ConsoleFullAccess política da Amazon.	13 de julho de 2023

Suporte adicionado para unir máquinas virtuais de armazenamento existentes a um Active Directory	Você pode unir máquinas virtuais de armazenam ento existentes a um Active Directory usando a AWS Management Console API AWS CLI e. Para obter mais informações, consulte Junção de uma SVM com um Active Directory.	13 de junho de 2023
Support para cache de NVMe leitura adicionado para sistemas de arquivos Single-AZ	NVMe O cache de leitura agora é compatível com sistemas de arquivos Single-AZ criados após 28 de novembro de 2022 com pelo menos 2% GBps da capacidad e de taxa de transferência na região Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda). Para obter mais informações, consulte Impacto do tipo de implantação na performance.	28 de novembro de 2022
Suporte adicionado para o uso de intervalos de endereços IP na VPC para criar sistemas de arquivos com várias AZs	Agora você pode criar sistemas de arquivos Multi-AZ FSx para ONTAP especific ando endpoints que estão dentro do intervalo de endereços IP da sua VPC. Para obter mais informações, consulte Criação FSx para sistemas de arquivos ONTAP.	28 de novembro de 2022

Suporte adicionado para atualizar tabelas de rotas de VPC em sistemas de arquivos com várias AZs	Agora você pode associar (adicionar) uma nova tabela de rotas de VPC a um sistema de arquivos Multi-AZ FSx para ONTAP existente ou desassociar (remover) uma tabela de rotas de VPC existente de um sistema de arquivos Multi-AZ for ONTAP existente. FSx Para obter mais informações, consulte Atualização de um sistema de arquivos.	28 de novembro de 2022
Support adicionado para criptografia de dados em trânsito com o AWS Nitro System	Os dados em trânsito são criptografados automatic amente quando acessados a partir de EC2 instâncias compatíveis da Amazon na região Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda). Para obter mais informações, consulte Criptografando dados em trânsito com o AWS Nitro System.	28 de novembro de 2022

Suporte adicionado para criar volumes DP	Agora você pode criar volumes DP (proteção de dados) usando o FSx console da Amazon AWS CLI ou a API da Amazon. FSx Você pode usar volumes DP como destino de um SnapVault relacionamento NetApp SnapMirror ou quando quiser migrar ou proteger os dados de um único volume. Para obter mais informações, consulte Tipos de volume.	28 de novembro de 2022
Suporte adicionado para copiar tags de volume para backups	Agora você pode habilitar `CopyTagsToBackups` na FSx API AWS CLI ou na Amazon a cópia automátic a de tags de seus volumes para backups. Para obter mais informações, consulte Cópia de tags para backups.	28 de novembro de 2022

Suport adicionado para escolher uma política de snapshot	Agora você pode escolher entre três políticas de snapshot integradas ao criar ou atualizar um volume usando o FSx console da Amazon ou a FSx API da Amazon. AWS CLI Você também pode selecionar uma política de snapshot personalizada que criou na CLI ou na API REST do ONTAP. Para obter mais informações, consulte Políticas de snapshot.	28 de novembro de 2022
Suporte adicionado para mais opções de capacidade de throughput do sistema de arquivos	FSx para ONTAP agora suporta 4.096 MBps de capacidade de taxa de transferência para sistemas de arquivos criados após 28 de novembro de 2022 na região Leste dos EUA (Ohio), Região Leste dos EUA (Norte da Virgínia), Região Oeste dos EUA (Oregon) e Europa (Irlanda). Para obter mais informações, consulte Impacto da capacidade de throughput na performance.	28 de novembro de 2022

Suporte adicionado para mais IOPS de SSD	FSx para ONTAP agora oferece suporte a 160.000 SSD IOPS para sistemas de arquivos criados após 28 de novembro de 2022 na região Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia) , Oeste dos EUA (Oregon) e Europa (Irlanda). Para obter mais informações, consulte Impacto da capacidade de throughput na performance.	28 de novembro de 2022
Support adicionado FSx para uso do ONTAP como um armazenamento de dados externo para o Cloud on VMware AWS	Você pode usar o FSx ONTAP como um armazenamento de dados externo para o VMware Cloud on AWS Software-Defined Data Centers (). SDDCs Esse suporte adicional fornece flexibilidade para aumentar ou diminuir o armazenamento, independe ntemente dos recursos de computação para cargas de AWS trabalho do VMware Cloud on. Para obter mais informações, consulte Usando o VMware Cloud with FSx for ONTAP.	30 de agosto de 2022

Aumentar automaticamente a capacidade de armazenamento de um sistema de arquivos	Use um AWS CloudFormation modelo personalizável AWS desenvolvido para aumentar automaticamente a capacidade de armazenamento do seu sistema de arquivos quando a quantidade de capacidade de armazenamento SSD usada exceder um limite especificado por você. Para obter mais informações, consulte Aumento da capacidade de armazenamento SSD dinamicamente.	3 de junho de 2022
A Amazon agora FSx está integrada com AWS Backup	Agora você pode usar AWS Backup para fazer backup e restaurar seus sistemas de FSx arquivos, além de usar os FSx backups nativos da Amazon. Para obter mais informações, consulte Usando AWS Backup com a Amazon FSx.	18 de maio de 2022
Suporte adicionado para implantações de sistemas de arquivos do ONTAP com uma única zona de disponibilidade	Você pode criar sistemas de arquivos Single-AZ FSx para ONTAP, que são projetados para fornecer alta disponibilidade e durabilidade em uma única Zona de Disponibilidade (AZ). Para obter mais informações, consulte Escolha da implantação do sistema de arquivos.	13 de abril de 2022

Support adicionado para AWS PrivateLink endpoints de interface VPC	Agora você pode usar endpoints VPC de interface para acessar a FSx API da Amazon a partir da sua VPC sem enviar tráfego pela Internet. Para obter mais informações, consulte Amazon FSx e a interface de VPC endpoints.	5 de abril de 2022
Suporte adicionado para modificar a capacidade de throughput dos sistemas de arquivos do ONTAP existentes	Agora você pode modificar a capacidade de throughput que está disponível para seus sistemas de arquivos do ONTAP existentes. Para obter mais informações, consulte Como gerenciar a capacidade de throughput.	30 de março de 2022
Suporte adicionado para capacidade de armazenamento SSD e escala de IOPS provisionadas	Agora você pode aumentar a capacidade de armazenamento SSD e as IOPS provisionadas dos sistemas de arquivos ONTAP existentes FSx à medida que seus requisitos de armazenamento e IOPS evoluem. Para obter mais informações, consulte Gerenciamento da capacidade de armazenamento e IOPS provisionadas	25 de janeiro de 2022

Support adicionado para CloudWatch métricas da Amazon	Você pode monitorar seu sistema de arquivos usando a Amazon CloudWatch, que coleta e processa dados brutos do FSx ONTAP em métricas legíveis e quase em tempo real. Para obter mais informações, consulte Monitoramento com a Amazon CloudWatch.	19 de janeiro de 2022
Suporte adicionado para mais opções de throughput do sistema de arquivos	FSx para ONTAP agora oferece suporte a 128 MBps e 256 MBps opções de taxa de transferência do sistema de arquivos. Para obter mais informações, consulte Impacto da capacidade de throughput na performance.	30 de novembro de 2021
O Amazon FSx for NetApp ONTAP agora está disponível ao público em geral	FSx for ONTAP é um serviço totalmente gerenciado que fornece armazenam ento de arquivos altamente confiável, escalável, de alto desempenho e rico em recursos, incorporado ao sistema de arquivos ONTAP. NetApp Ele fornece os recursos, o desempenho, os recursos e os sistemas APIs de NetApp arquivos familiare s com a agilidade, a escalabil idade e a simplicidade de um serviço totalmente gerenciado AWS .	2 de setembro de 2021

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.